Docket No.: 050108-0061 **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	Customer Number: 20277
Varsha CLARE, et al.	:	Confirmation Number: 6881
Application No.: 10/695,805	:	Group Art Unit: 2686
Filed: October 30, 2003	:	Examiner: Khawar IQBAL

For: OPTIMIZED NETWORK EMPLOYING SEAMLESS AND SINGLE SIGN ON CAPABILITIES FOR USERS ACCESSING DATA APPLICATIONS ON DIFFERENT NETWORKS

DECLARATION OF INVENTORS ALLEN BILLINGS AND KENT HUGHES, UNDER 37 C.F.R § 1.131

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

1. Along with Varsha Clare, we Allen Billings and Kent Hughes, are the inventors of the patent application identified above and of the subject matter described and claimed therein.

2. Varsha Clare is no longer an employee of the Assignee, Cellco Partnership (d/b/a Verizon Wireless).

3. Our invention as described and claimed in the subject application was completed in this country prior to May 5, 2003, as evidenced by the following:

A) Prior to May 5, 2003, the inventors prepared a document entitled "Verizon Wireless Authentication, Authorization and Single Sign-on for Data Products and

Services," Version 1.2. Attached Exhibit 1 is a true copy of that document. The cover page of the document bears a date. The date has been redacted. The date on the cover page of the "Verizon Wireless Authentication, Authorization and Single Sign-on for Data Products and Services" document (Exhibit 1) is prior to May 5, 2003.

B) Prior to May 5, 2003, the inventors prepared a document entitled "Authentication, Authorization and Single Sign-on for Data Products and Services" (without version number). Attached Exhibit 2 is a true copy of that document. The cover page of the document bears a date. The date has been redacted. The date on the cover page of Exhibit 2 is prior to May 5, 2003.

C) Prior to May 5, 2003, the inventors prepared a document entitled "Discussion Points – Authentication and Authorization for VZW Products." Attached Exhibit 3 is a true copy of that document. This document bears no date.

D) Prior to May 5, 2003, the inventors completed a Verizon Wireless Invention Disclosure form regarding our invention, then entitled "Authentication/Single Sign On." Attached Exhibit 4 is a true copy of that Verizon Wireless Invention Disclosure. The second page of the Verizon Wireless Invention Disclosure form regarding our invention lists a conception date. That date, which has been redacted, is prior to May 5, 2003. The third page of this form identifies two detailed description documents by file names, which documents correspond to the documents in Exhibits 2 and 3. The dates associated with those document citations in the Verizon Wireless Invention Disclosure form, which have been redacted, are prior to May 5, 2003.

4. From a date prior to May 5, 2003 until October 30, 2003, we (all three inventors) continued to work toward deployment of a single sign-on for products and services offered by Verizon Wireless.

(i) For example, Allen Billings prepared a document, and solicited comments on the document from at least the other inventors, which document was entitled "Single Sign-on Third-Party Authorization Vendor and Platform Recommendation," a true copy of which is attached hereto as Exhibit 5. The cover page of this document (Exhibit 5) bears a May 7, 2003 date.

(ii) Allen Billings also prepared a document, and solicited comments on the document from at least the other inventors, which document was entitled "Single Sign-on Third Party Authorization Requirements," Version 1.2 (DRAFT), a true copy of which is attached hereto as Exhibit 6. The cover page of the document (Exhibit 6) bears a May 21, 2003 date. Dates for two earlier revisions listed on page 2 of the document (Exhibit 6), which have been redacted, are prior to May 5, 2003.

(iii) During at least part of 2003, the Verizon Wireless internal name for the relevant project was "Product Authentication." Exhibit 7 is a true copy of a printout of the "Verizon Wireless Product Authentication Project Plan" (file name "Product Authentication Project Plan v1.0.xls"), which was a high-level project plan that shows the planned dates for deploying the Product Authentication for three different Verizon Wireless services: Multimedia Messaging Service (MMS), Wireless Internet Browser (WAP2) and Push to Talk (PTT). The Project Plan (Exhibit 7) is dated June 6, 2003 and lists projected action dates spanning the Summer of 2003.

(iv) Allen Billings and another Verizon Wireless employee prepared a document, describing our on-going work, entitled "Product Authentication (LDAP) Architecture for Alarming Scenarios" (DRAFT) a true copy of which is attached hereto as Exhibit 8. This document shows Verizon Wireless's plan for deploying Product Authentication in a way that would minimize failures on the network. The cover page of this document (Exhibit 8) bears a date of June 20, 2003.

(v) Allen Billings prepared a document, describing our on-going work, entitled "Product Authentication Roaming Issues" a true copy of which is attached hereto as Exhibit 9. This document describes some issues related to roaming, which were discovered during the process of deploying Product Authentication, along with several possible solutions. The cover page of this document (Exhibit 9) bears a date of September 2, 2003.

5. From a date prior to May 5, 2003 until October 30, 2003, we (all three inventors) worked with David Tennant of the DC office of McDermott Will & Emery LLP to facilitate the preparation and filing of the above-identified patent application. For example, we provided copies of the documents attached as Exhibits 5 and 6 to David Tennant for his consideration in drafting the above-identified application. As another example, we also reviewed and provided comments on one or more drafts of the application in August and September of 2003. We, Allen Billings and Kent Hughes, have reviewed the declaration by Keith E. George and the Exhibits accompanying that declaration. We believe that the description of the disclosure and the application preparation, in the George declaration is accurate.

6. Our application, as identified above, was filed on October 30, 2003.

Application No.: 10/695,805

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

January 11, 2006
Date

Allen Billings

January 11, 2006
Date

Kent Hughes

verizon wireless

Verizon Wireless

Authentication and Single Sign-on for Data Products and Services

Version 1.2

Network Technology Development

[redacted]

RESTRICTED AND PROPRIETARY

The information contained herein is for use by authorized Verizon Wireless & subsidiaries employees with a need to know it and should not be disclosed to others.

Table of Contents

Executive Summary - Authentication and Single Sign-On for Verizon Wireless Data Products

- **OBJECTIVE:** Investigate a <u>common</u> solution for Verizon Wireless data products to meet the following requirements
  - **Identification:** Securely identify subscribers accessing data products through the wireless network to prevent unauthorized access to subscriber information and data.
  - **Authorization:** Authorize subscribers to access data products through the wireless network to prevent revenue leakage of provisioned products.
  - **Single Sign-on:** Introduce a common and single sign-on to Verizon Wireless products from a wireline computer interface to access user preferences and data.

- **EVALUATION**
  - Identification and Authorization solutions evaluated:
    - **Query into AAA Session Database:** The Product Servers query into the AAA's Session Database (by source IP address) for trusted identification of the subscriber (by MIN) each time a connection to the Product Server is made.
    - **Application-level security:** An authentication key is provisioned in the device and server, and is used to perform authentication. The authentication can be managed by a single network element on behalf of the individual product servers (single key), or the authentication can be managed separately by the product servers (multiple keys required).
  - Single Sign-on solution evaluated:
    - **HTTP Redirect:** A common database is used to store username (MDN) and password information for all subscribers that have signed up for any of the relevant Verizon Wireless products (e.g. Push-to-talk, Voice Portal/Unified Messaging, Vtext). After authentication from this database, users are connected to individual products through HTTP Redirects with the username encrypted in the URL.

- **RECOMMENDATION**
  - **Identification and Authorization:** Implement the Query into AAA Session Database method for wireless identification and authorization.
  - **Single Sign-on:** Implement HTTP Redirect method, initially using the TCS Vtext platform as the Central Database.

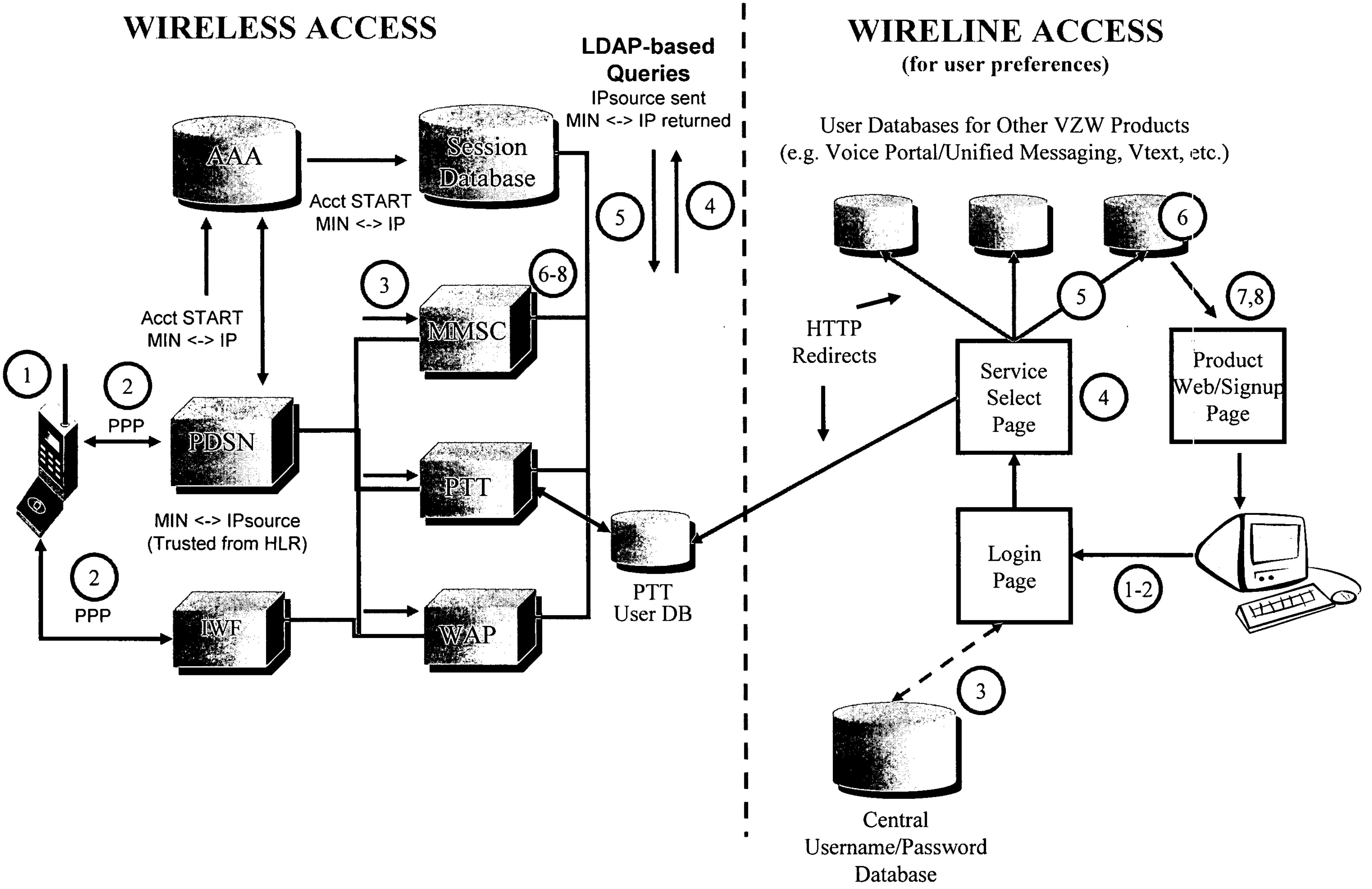
Architectural Description
Session Database Query for Identification and Authorization

- **Overview – Session Database Query**
  - AAA Server has a trusted mapping of MIN to source IP address, based on HLR A-key authentication.
  - Product Servers can use this mapping to verify identification of the subscriber. Requests for service from the handset are routed to the product server using TCP/IP, and therefore have an associated IP address. The software client in the device imbeds the MIN in the data packet of this request. A query to the Session Database will verify that the MIN in the data packet is correctly associated with the IP address of the request.
- **Setup Requirements for Session Database Query**
  - Client: MIN or MIN-based client ID must be included in connection requests to Product Servers (required for identification under all scenarios).
  - AAA Server: Must forward accounting start and stop records to Session Database.
  - Session Database
    - Must keep a record of all active 1X data sessions, including a mapping of MIN to source IP address.
    - Must support LDAP-based queries, returning the MIN to IP mapping when queried with IP address.
  - Product Servers: Must support LDAP queries to obtain MIN to IP mapping, and make authorization decisions accordingly.
- **Connection process – wireless access through local client on the device (see Network Diagram – pg 6)**
  1. User launches the specific product or service (PTT, WAP, MMS, etc)
  2. Client imbeds MIN (or MIN-based Client ID) into IP request packet and sends to Product Server
  3. Product Server receives packet and checks provisioned database. If MIN is provisioned, then Product Server proceeds with providing service. If not, service is denied.
  4. Simultaneously, Product Server queries the Session Database by sending the source IP address of the request
  5. Session Database responds to query with MIN to IP mapping or a value of "FALSE" if the IP address is not found in the database (this will occur if the subscriber is using QNC).
  6. 1X Connections: If MIN to IP mapping matches that of the request then Product Server, then it indicates that the connection is over 1X. Product Server continues to allow service.
  7. 1X Connections: If MIN to IP mapping is different than that of the request, then the connection is fraudulent and the Product Server stops service.
  8. IS95 Connections: If Session Database returns "IP Not Found", it means the user has connected through IS95 and the Product Server continues to allow service (I.e. service is allowed for all QNC connections. However, a fraudulent user cannot retrieve user data without additional application-layer sign-on.).

Architectural Description
HTTP Redirects for Single Sign-on

- **Overview – Single Sign-on**
  - Users log in to a Central Database (initially provided by TCS Vtext platform)
  - HTTP Redirects are used to pass encrypted Username (MDN-based) to individual Product Servers
- **Setup requirements for Single Sign-on to user preferences and data**
  - Product Servers: Users must be provisioned as usual
  - Central Database: self-registration process
    - Web-based login page includes an option for "New User"
    - User enters MDN and any required data
    - An entry is made for the user in the Central Database, and a temporary password is generated by the Central Database
    - SMS message with the temporary password is sent based on the MDN entered by the user
    - User is prompted to change the password, and can now access appropriate products
  - Central Database: automatic-registration process (requires provisioning development)
    - Provisioning system notifies central database when a subscriber (either new or existing) registers for a Verizon Wireless product that has wireline login capability.
    - If there is not a record for the subscriber in the Central Database, a new entry is made, and a temporary password is sent via SMS
    - If there is already a record for the subscriber in the Central Database, nothing is done
    - The user can login using the temporary password, and will be prompted to change the password
- **Connection process – wireline single sign-on to user preferences and data (see diagram – pg 6)**
  1. User launches URL for desktop interface to Verizon Wireless products, and is given a login Web-page.
  2. User enters Username (MDN or user-selected username) and Password.
  3. Username and Password is authenticated by a central database, and a "Service Select" page is displayed with links to the individual products (The actual layout and flow of Web pages is flexible – a generic approach is presented here).
  4. User selects a product to connect to by clicking on the appropriate link.
  5. An HTTP Redirect sends encrypted MDN to the appropriate Product Server.
  6. Product Server checks in its local database to validate that the user has subscribed to the service.
  7. If the user is authorized to use the service, they are presented with the service's Web-page.
  8. If the user is not authorized to use the service, they can be given an opportunity to sign up, or provided with information about the service and a number they can call to sign up.

Network Diagram



WIRELESS ACCESS

WIRELINE ACCESS

(for user preferences)

AAA

Session Database

Acct START
MIN <-> IP

Acct START
MIN <-> IP

LDAP-based Queries
IPsource sent
MIN <-> IP returned

PPP

PDSN

MIN <-> IPsource
(Trusted from HLR)

PPP

IWF

MMSC

PTT

WAP

PTT
User DB

User Databases for Other VZW Products
(e.g. Voice Portal/Unified Messaging, Vtext, etc.)

HTTP
Redirects

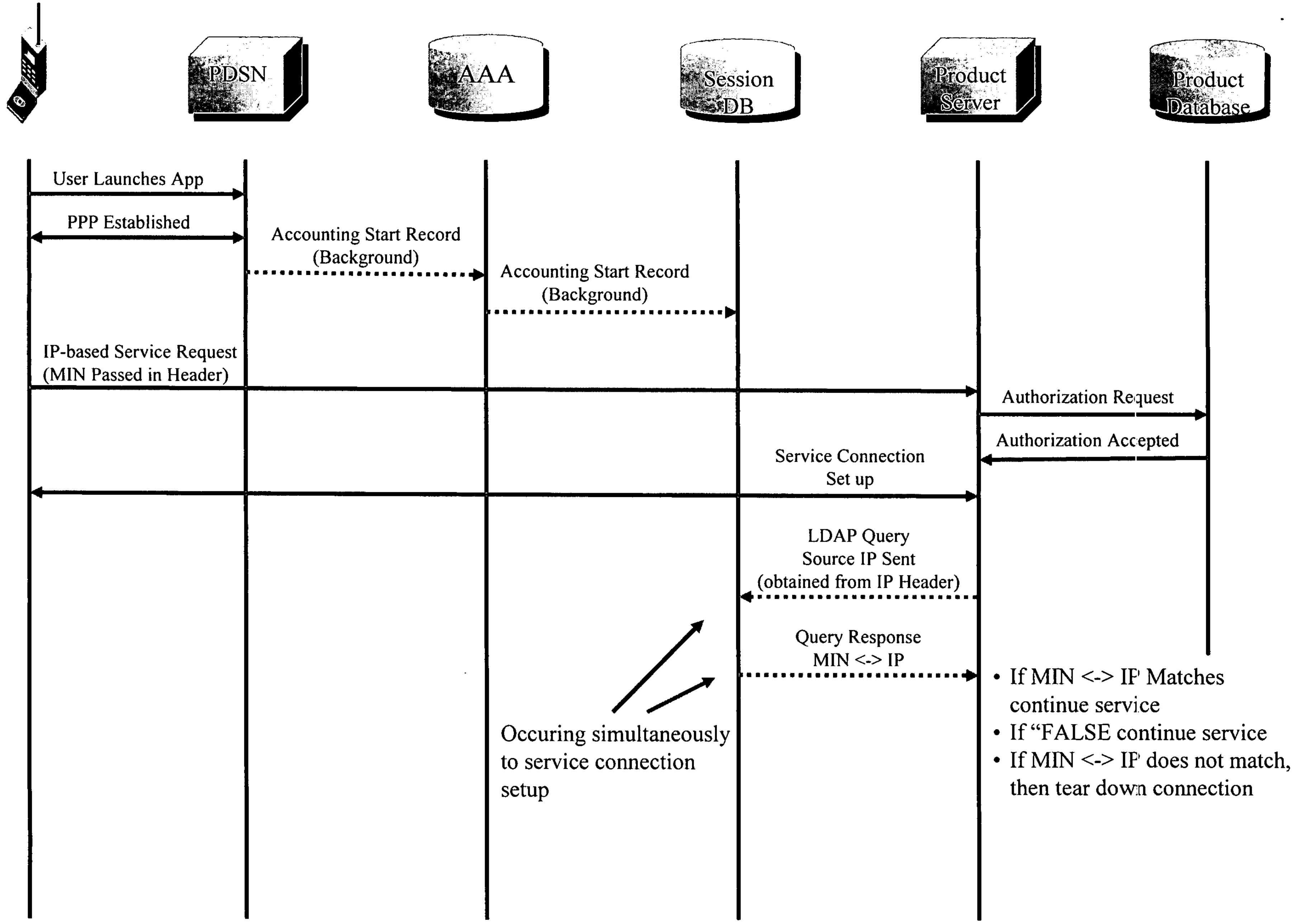
Service Select Page

Product Web/Signup Page

Login Page

Central Username/Password Database

Call Flow - Session Database Query for 1XRTT Connections



PDSN

AAA

Session DB

Product Server

Product Database

User Launches App

PPP Established

Accounting Start Record (Background)

Accounting Start Record (Background)

IP-based Service Request (MIN Passed in Header)

Authorization Request

Authorization Accepted

Service Connection Set up

LDAP Query Source IP Sent (obtained from IP Header)

Query Response MIN <-> IP

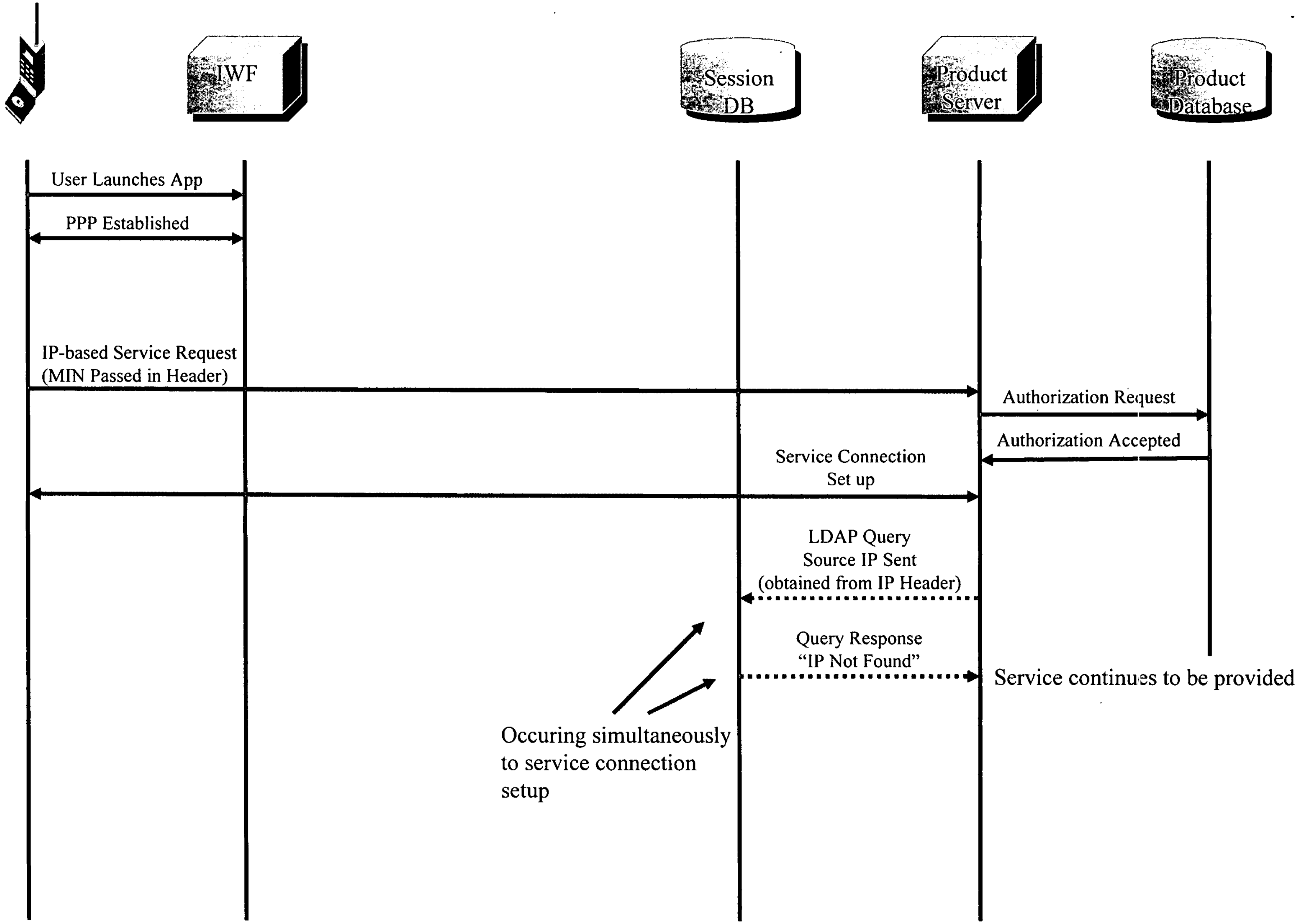
Occuring simultaneously to service connection setup

- If MIN <-> IP Matches continue service
- If "FALSE continue service
- If MIN <-> IP does not match, then tear down connection

RESTRICTED AND PROPRIETARY

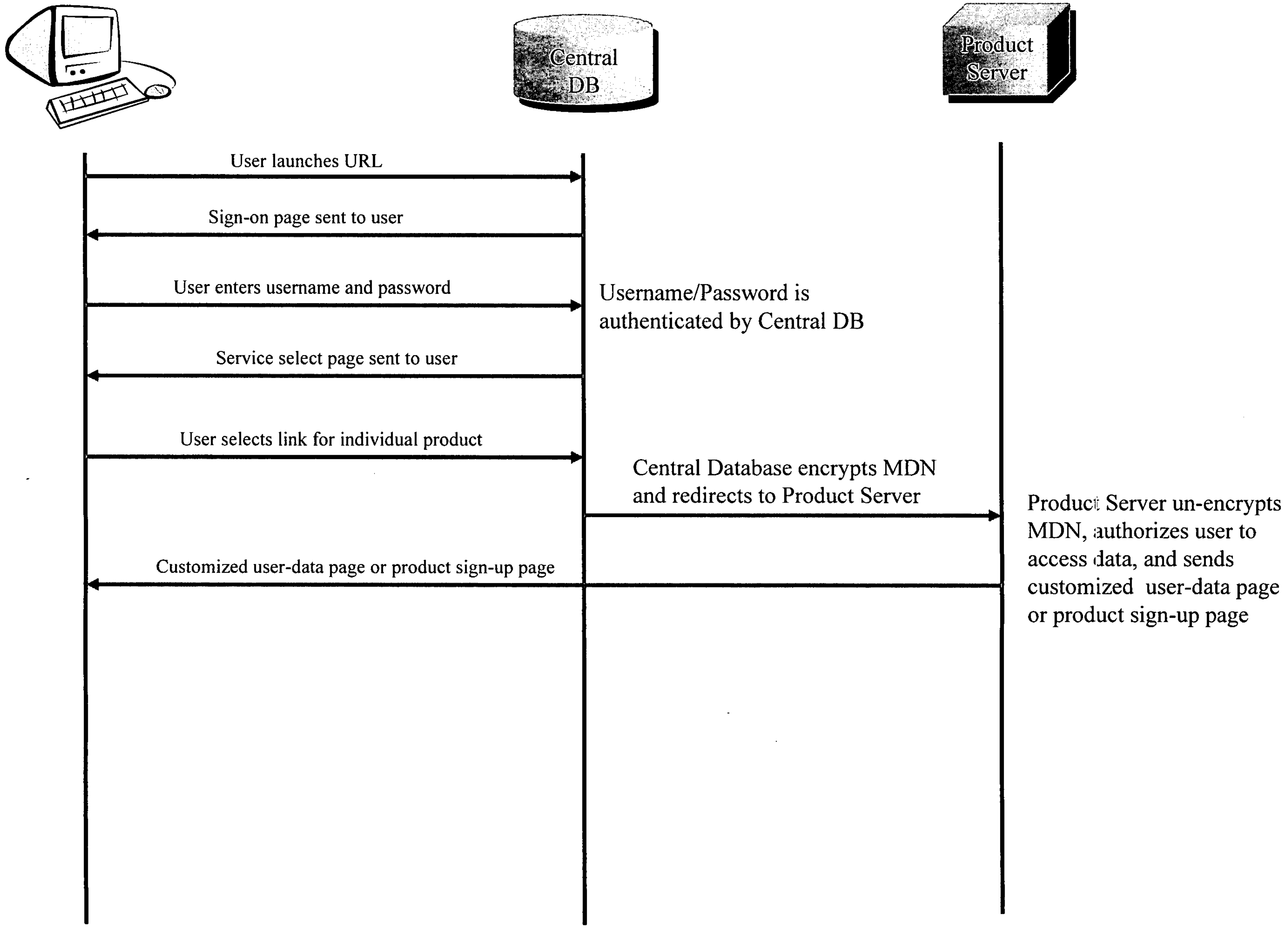
The information contained herein is for use by authorized Verizon Wireless employees with a need to know it and should not be disclosed to others.

Call Flow - Session Database Query for IS95 Connections


IWF
Session DB
Product Server
Product Database
User Launches App
PPP Established
IP-based Service Request (MIN Passed in Header)
Authorization Request
Authorization Accepted
Service Connection Set up
LDAP Query Source IP Sent (obtained from IP Header)
Query Response "IP Not Found"
Service continues to be provided
Occuring simultaneously to service connection setup

RESTRICTED AND PROPRIETARY
The information contained herein is for use by authorized Verizon Wireless employees with a need to know it and should not be disclosed to others.

Call Flow – HTTP Redirects



User launches URL

Sign-on page sent to user

User enters username and password

Username/Password is authenticated by Central DB

Service select page sent to user

User selects link for individual product

Central Database encrypts MDN and redirects to Product Server

Product Server un-encrypts MDN, authorizes user to access data, and sends customized user-data page or product sign-up page

Customized user-data page or product sign-up page

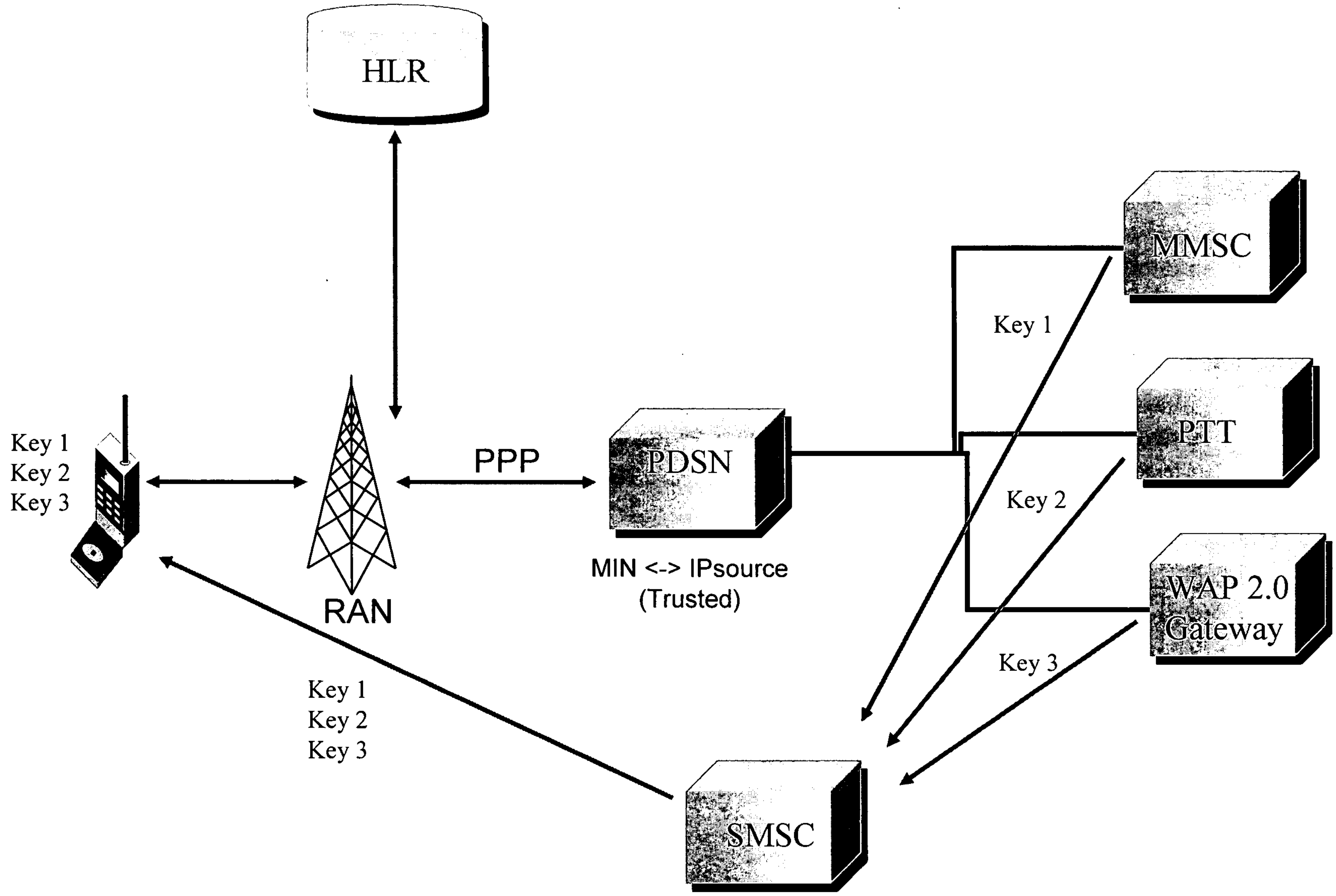
Next Steps

- Overall
  - Reach consensus on end-to-end solution
  - Receive buy-in from key stakeholders
  - Identify responsible parties for implementation of the full project
- Session Database
  - Finalize query protocol to verify that LDAP is the best approach
  - Program management of the implementation and testing of Ericsson RMS Session Database
- Product Servers
  - Communicate detailed requirements to appropriate vendors for both Session Database Queries and HTTP Redirect integration
  - Program management of the implementation and testing of end-to-end solution
- Central Database
  - Finalize decision to use TCS platform for Central Database
  - Reach consensus on long-term direction
  - Communicate detailed requirements to appropriate vendors
  - Program management of the implementation and testing of end-to-end solution

Appendix – Synopsis of Application-level Authentication

- Overview: An authentication key is used to perform authentication.
- Process – new user or new device
  - User attempts to initiate a new session to Product Server
  - Product Server detects that the request is from a new user and generates a secret key
  - Key is imbedded in an SMS message and sent to the device
  - Device attempts new session using the secret key
  - Product Server authenticates subscriber with matching key (based on standard authentication algorithm)
- Future connections use existing secret key for authentication. Key updates may take place by regenerating key, and distributing via SMS.
- Alternative implementation: move authentication function out of Product Servers into separate network network element to allow single authentication key. Centralized authentication "server" would forward authenticated traffic to Product Servers.
- Development Effort:
  - Product Server development or new network element necessary to generate and distribute keys.
  - Devices: Must support storage and use of key(s). Must interpret incoming SMS message containing secret key and store locally.
- Pros
  - More secure, and could be used to support encryption
  - Better performance – no per-session queries
  - Supports IS95 with no additional modifications
  - Others?
- Cons
  - Dependent on device and server development – time to market concern
  - Either devices must support multiple keys, or a new network element must be developed and deployed

Appendix – Network Diagram of Application-level Authentication



Authentication, Authorization and Single Sign-on for Data Products and Services

Network Technology Development

[redacted]

RESTRICTED AND PROPRIETARY

The information contained herein is for use by authorized Verizon Wireless & subsidiaries employees with a need to know it and should not be disclosed to others.

Authentication, Authorization and Single Sign-On: Objectives

- Investigate a single common Authentication, Authorization, and Sign-on solution for Verizon Wireless products.

- Customer Experience Objectives:
  - Allow users to sign on to any VZW product using the same username/password combination.
  - Eliminate need to enter username/password whenever it is not necessary for security.
  - Provide level of security that users can trust.

- Network Objectives:
  - Leverage robust A-key authentication
  - Leverage AAA functionality
  - Consolidate diverse but common network solutions
  - Simplify provisioning
  - Simplify network interface requirements for Product Servers

Authentication, Authorization and Single Sign-On: Key Requirements

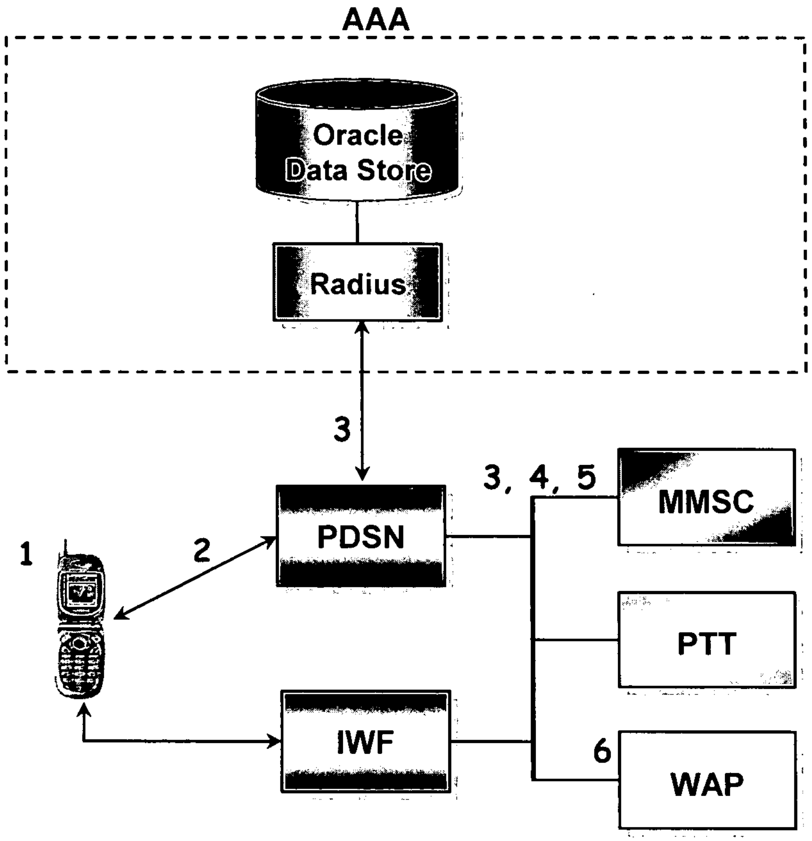
- ○ Authentication of wireless device client
  - — HTTP based clients (WAP, PTT, MMS) present MIN as client (or subscriber identity).
  - — Need to assure that the MIN is not spoofed.

- ○ Authentication of user that accesses application via web (anonymous terminal).
  - — Applications such as PTT and vtext require user access via web (to set up & modify profile).
    - Required functionality:
      - Support Web interface for user to enter username and password
      - Provide a method for user to manage the password.
      - For a user that does not yet have a Web login password, generate a temporary password and send it to the user in an SMS message.
  - — Single sign-on (user name, password) for all Verizon Wireless products including 1X, 802.11, PTT, EVDO, MMS and vtext would simplify subscriber interface.

- ○ Authorize use of a product – 1X, 802.11, PTT, MMS, etc.
  - — Two types of authorizations
    - Basic: Product server needs to verify that the user is authorized to use the service, e.g., 1X, 802.11, WAP.
    - Service Type: In addition to basic authorization, product server needs to know service type (level of service) subscribed. Example product: Multiple Bundles.

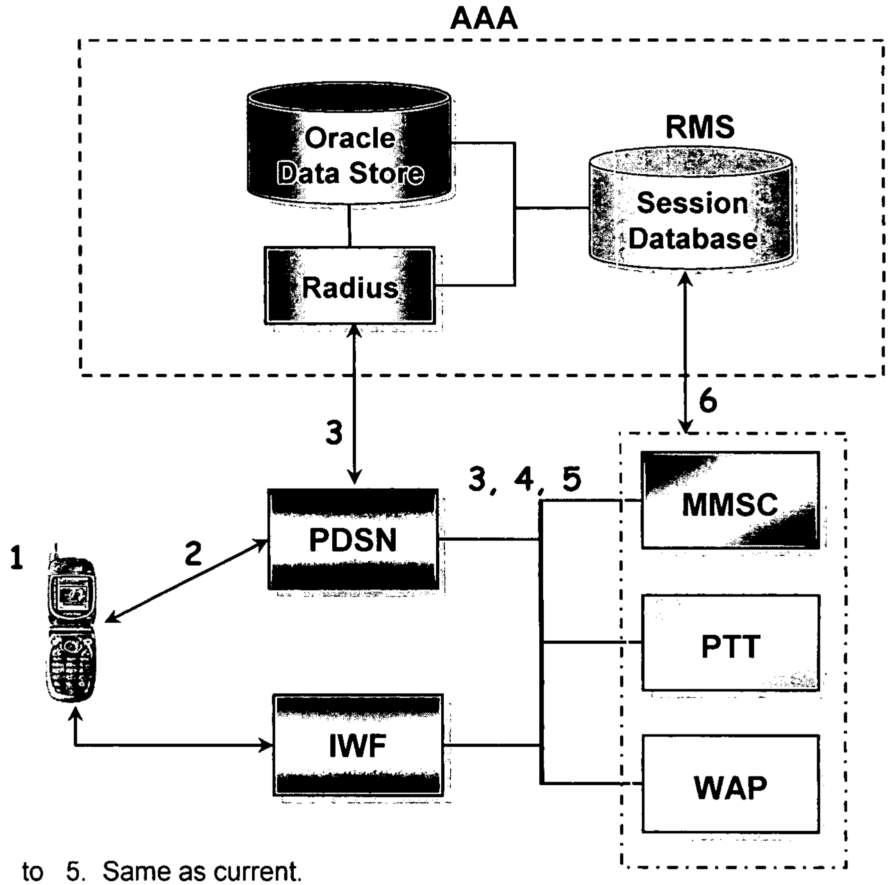
Authentication of Wireless Device

Current



1. User launches application.
2. PDSN receives A-Key authenticated MIN over RP interface.
3. PDSN sets up data session between handset and product server. AAA and PDSN aware of MIN & IP address.
4. Product server receives MIN from the client in handset.
5. Product Servers cannot trust the MIN (may be spoofed).
6. Currently, WAP gateway uses additional key to authenticate MIN. PTT & MMS will accept MIN as given by the client.

Using AAA Session Database



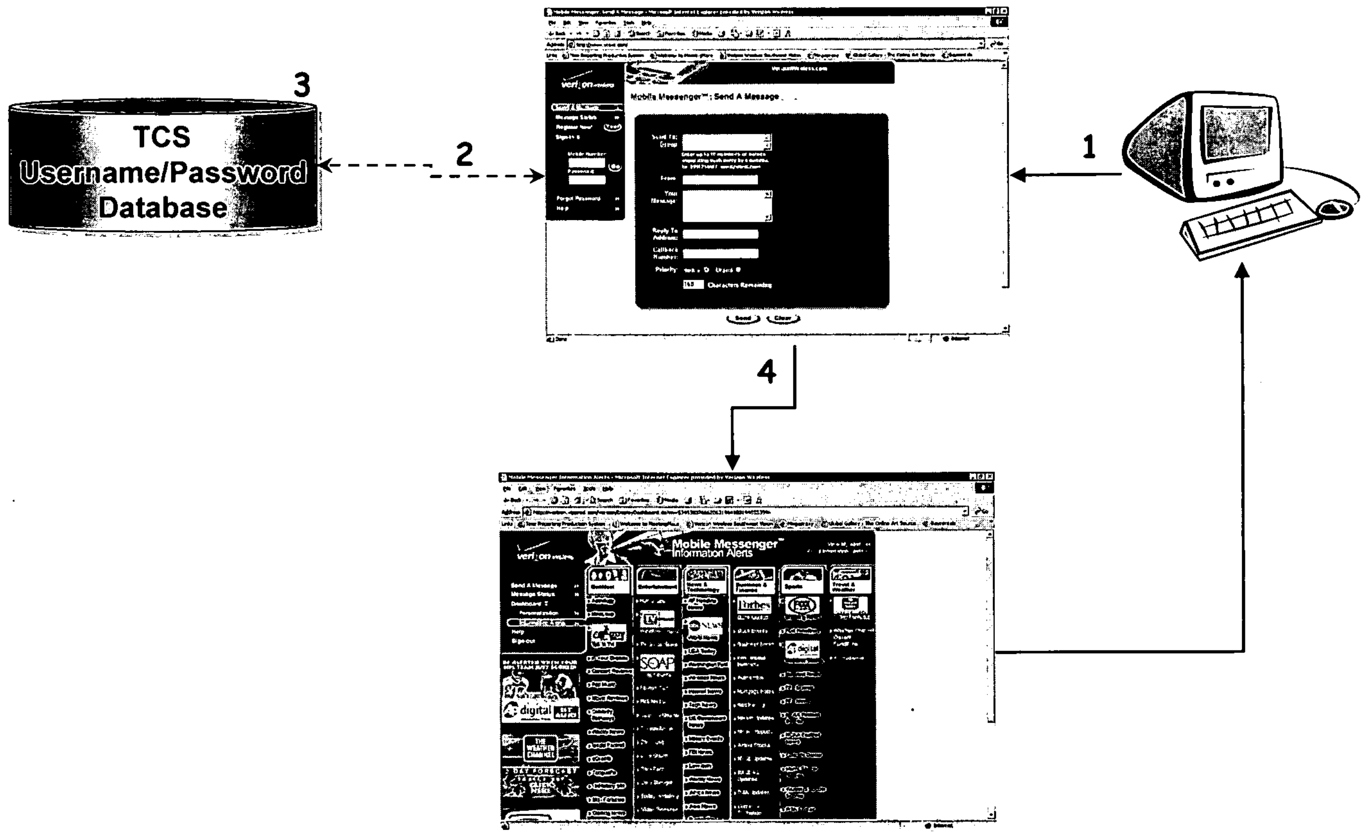
1. to 5. Same as current.
6. Product Server queries session database and obtains trusted MIN to authenticate client.

Highlights:

- Session database is currently part of Ericsson Bridgewater AAA.
- Verizon Wireless has purchased this functionality.
- This is the standard process used by Product Servers in GSM.

RESTRICTED AND PROPRIETARY
The information contained herein is for use by authorized Verizon Wireless employees with a need to know it and should not be disclosed to others.

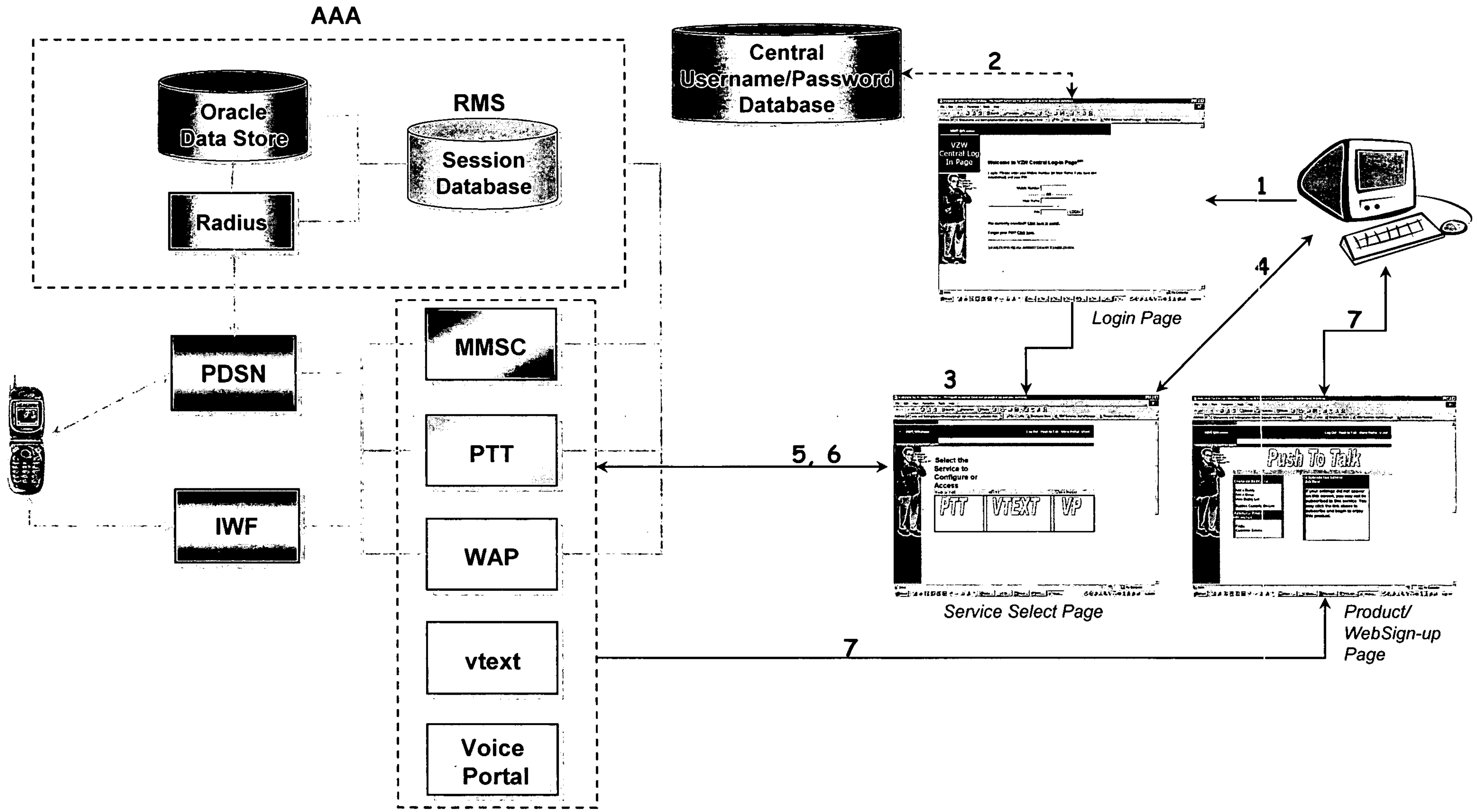
Authentication for Web Access: vtext.com


3
TCS
Username/Password
Database
2
1
4
Mobile Messenger™: Send A Message
Mobile Messenger™ Information Alerts

1. User goes to vtext.com and enters user name and password.
2. TCS web application provides user name password management.
3. TCS database stores user name & password.
4. TCS web application provides http redirect with user name password to Vodafone.

RESTRICTED AND PROPRIETARY
The information contained herein is for use by authorized Verizon Wireless employees with a need to know it and should not be disclosed to others.

Authentication and Single Sign-On for Web Access: Future



1. User links to VZW Products and enters username and password
2. Login authenticated by central database (TCS) or AAA
3. Menu of VZW products displayed
4. User selects a product
5. HTTP redirect sent with Username/password to Product Server
6. Product Server checks if user is provisioned
7. User is logged in or given opportunity to sign up for service

Highlights:
- TCS application developed for vtext.com.
- PTT application is looking at using TCS.
- TCS needs to make several changes to support PTT.
- Cannot be used for 802.11 (without AAA integration).

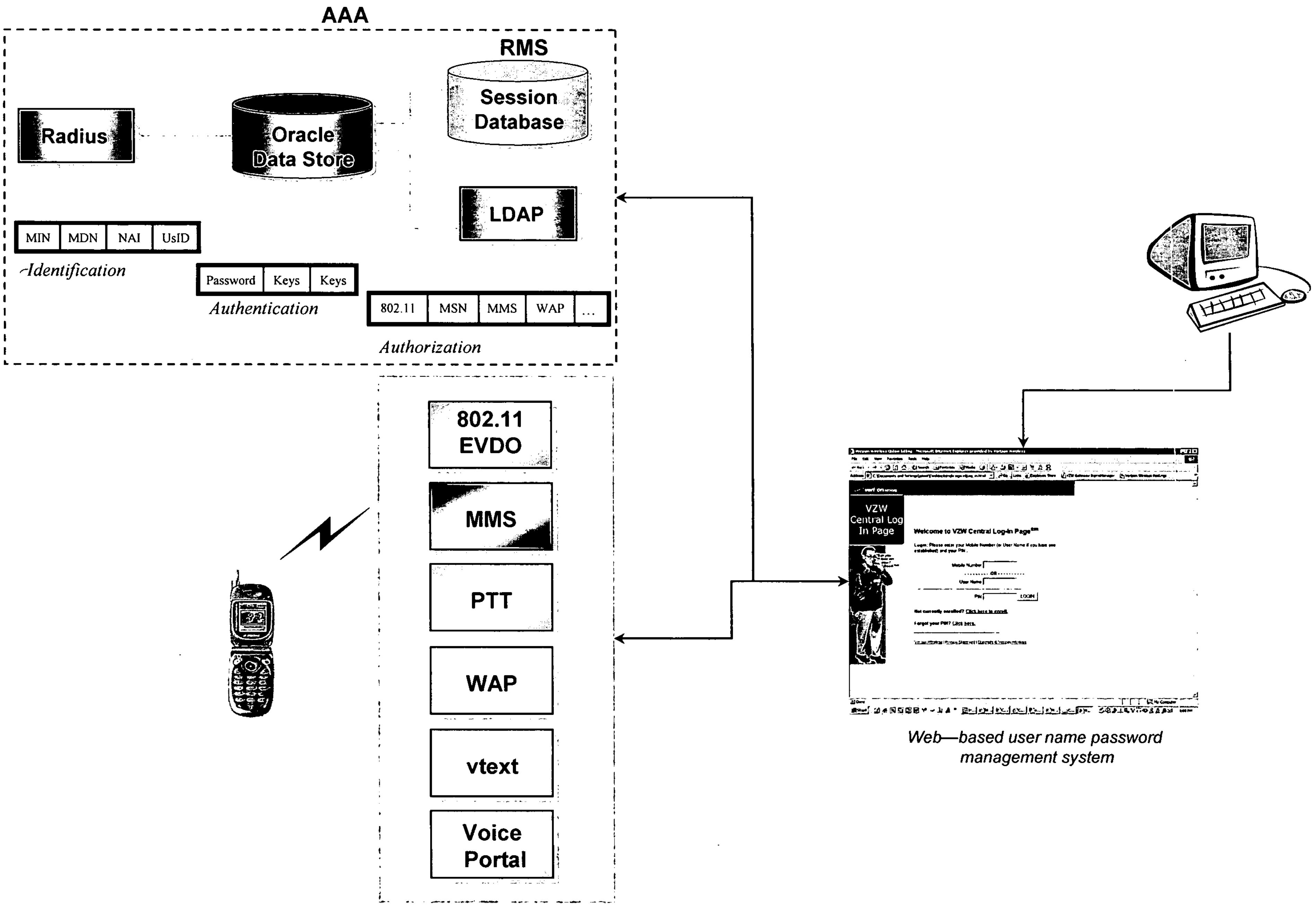
Single Sign-On: Web-Based Password Management

- ❍ Currently, vtext.com has a web-based user name, password management system.

- ❍ Two options:
  - — Option 1 – TCS front-end, AAA data store
    - Expand vtext.com web server to include all products, including 802.11.
    - Store the user name and password in the AAA data store.

  - — Option 2 – AAA front-end, AAA data store
    - Develop user name password process for AAA to support 802.11.
      - Ericsson Bridgewater AAA currently provides this functionality.
        - Need Verizon Wireless adaptation (web page design).
    - Eliminate vtext.com user name password method and database.

Authentication, Authorization and Single Sign-On: Centralized Database - Concept



Web—based user name password management system

RESTRICTED AND PROPRIETARY
The information contained herein is for use by authorized Verizon Wireless employees with a need to know it and should not be disclosed to others.

A Few Thoughts on LDAP

- In the future, 3rd party applications and new products may require additional data fields that are common to many applications (note: these are not authentication and authorization fields).
- It may be preferred that these applications have LDAP interface available to the common store.
- LDAP and AAA data store will have some common data items.
- Ericsson-Bridgewater AAA claims to have LDAP interface available.
  - Not clear if this requires external LDAP directory (duplicated data or access to Oracle database via LDAP protocol).

Authentication, Authorization, Single Sign-On: Highlights

- ○ Must Do
  - — AAA Session Database for authentication of MMS, PTT, WAP clients.
  - — Common user name and password for PTT, vtext.com, 802.11, 1X, EVDO.
  - — AAA to authorize more than 1X.
    - 802.11
    - EVDO

- ○ Key Challenges
  - — All of the above need Network Planning Support.
    - AAA is central to all of these functions.
    - AAA is being impacted by other key feature, e.g., 1X, Prepay Data.

- ○ Topics of Intense Debate
  - — Role of AAA.
  - — Roles and responsibilities for authentication and authorization.
  - — Organization responsible for central data store.

RESTRICTED AND PROPRIETARY
The information contained herein is for use by authorized Verizon Wireless employees with a need to know it and should not be disclosed to others.

APPENDIX

Summary of Authentication and Authorization Requirements

- What Product Servers and Applications Need
  - Authentication
    - Wireless Device: Product Server needs to verify the identification of a user requesting service from a wireless device. Example products effected: WAP, PTT, MMS.
      - Required functionality: Product Server sends an originator's IP address, received in IP packet, to AAA (session database). AAA (session database) returns trusted MIN (received over R-P interface – authenticated MIN).
    - Web Access: Product Server needs to authenticate a user logging in for access to profile information stored on the Product Server. Products effected: PTT, vtext, Voice Portal, possibly WAP MMS or 802.11 in the future.
      - Required functionality:
        - Support Web interface for user to enter username and password
        - Provide a method for user to manage the password.
        - For a user that does not yet have a Web login password, generate a temporary password and send it to the user in an SMS message.
  - Authorization. Two levels of authorization:
    - Basic: Product Server needs to verify that the user is authorized to use the service.
      - Required functionality: AAA returns a yes/no value to Product Server indicating whether the user (based on NAI, MDN, MIN, user name or IP) is authorized to use the service. Example products affected: 802.11, 3rd Party Apps.
    - Service Type: Product Server or application has predefined service types (i.e. class of service), and needs to know which service type to use (example: Microsoft multiple bundles).
      - Required functionality: AAA performs basic authorization as described above, and returns service class or type. Example products affected: MS Multiple Bundles, 3rd Party Apps, and maybe WAP, PTT, and 802.11

Requirements for Individual Applications (See previous page for descriptions)

- MMS
  - Authentication
    - Wireless Device – yes (by MIN < -- > IP mapping)
    - Web Access – no (maybe in future)
  - Authorization
    - Basic – yes
    - Service Type – no
      (maybe in future)
- Push to Talk
  - Authentication
    - Wireless Device – yes (by MIN < -- > IP mapping)
    - Web Access – yes (for password management and profile access)
  - Authorization
    - Basic - yes
    - Service Type - maybe
- 802.11
  - Authentication
    - Wireless Device – yes (by NAI from roaming partner)
    - Web Access – yes (for password management only)
  - Authorization
    - Basic - yes
    - Service Type - maybe

Requirements for Individual Applications

- 3rd Party Applications (e.g. MSN Multiple Bundles)
  - Authentication
    - Wireless Device - no
    - Web Access – no (done through VZW-MSN)
  - Authorization
    - Basic - yes
    - Service Type – yes
- WAP
  - Authentication
    - Wireless Device – yes (by MIN < -- > IP mapping)
    - Web Access – not today
  - Authorization
    - Basic - yes
    - Service Type – maybe
- 1X
  - Authentication
    - Wireless Device – yes (by IS835)
    - Web Access – yes (for password management only)
  - Authorization
    - Basic – yes by IS835
    - Service type - no

Requirements for Centralized Single Sign-on Using AAA Server

- Information: The AAA must store the following information to be used for desired functionality
  - Subscriber Identification Information
    - MIN – provisioned by MTAS
    - MDN – provisioned by MTAS
    - NAI – generated based on provisioned MDN
    - User-ID – chosen by user
  - Authentication Information
    - 1X infrastructure Password – programmed into device (default today is “vzw”)
    - User-defined Password – chosen and entered by user
    - Authentication keys for MIP
  - Authorization Information – yes/no field provisioned by MTAS and a service type indicator (when required)
    - Services: 1X, EVDO, 802.11
    - Products: Vtext, PTT, WAP, MMS
    - 3rd Parties: MSN Multiple Bundles
- Functionality
  - Queries for authentication.
    - Wireless Device: Product Server sends originator’s IP address received in IP packet to AAA (session database). AAA (session database) returns MIN.
    - Web Access
      - Support Web interface for user to enter username and password and manage password
      - For a user that does not yet have a Web login password, generate a temporary password and send it to the user in an SMS message.
  - Queries for authorization information.
    - Basic: Product Server sends IP address, NAI, 802.11, MDN or user name. AAA returns yes or no to authorize.
    - Service Type: Product Server sends IP address, NAI, 802.11, MDN or user name. AAA returns a service type indicator.

Solution #1 – Authentication for Wireless Devices

- Authentication for Wireless Devices
  - PROBLEM STATEMENT
    - 1X Network relies on A-key authentication to identify subscriber
    - This identification is not passed downstream to Product Servers and applications
    - Product Servers know that the user has been authorized as a valid, paying Express Network subscriber, but they don't have trusted identification of the subscriber
  - GOAL: Leverage A-key authentication to securely identify the user at the Product Servers to avoid implementing unique authentication solutions by each Product Server.
  - SOLUTION: Query into the AAA Session Database
    - Session Database holds a list of active data sessions, which can be used for subscriber identification
    - When a request for service is made, Product Server begins providing service, while making a query (in the background) to the Session Database to verify identification of the subscriber.
    - Required functionality: Product Server sends an origination IP address, received in IP packet, to AAA (session database). AAA (session database) returns trusted MIN (received over R-P interface – authenticated MIN).
    - If subscriber identification matches, service simply continues. If subscriber identification does not match, then the Product Server discontinues tears down the session.
  - STATUS: Solution is currently being implemented
    - Session Database is part of the AAA RMS, which was purchased by VZW as part of the Express Network implementation.
    - Working with Ericsson/Bridgewater to finalize specifications for the Session Database query.
    - Working with Product Server vendors to implement query capability and authentication algorithm.

Solution #2 – Authentication and Single Sign-on of Anonymous Web Users

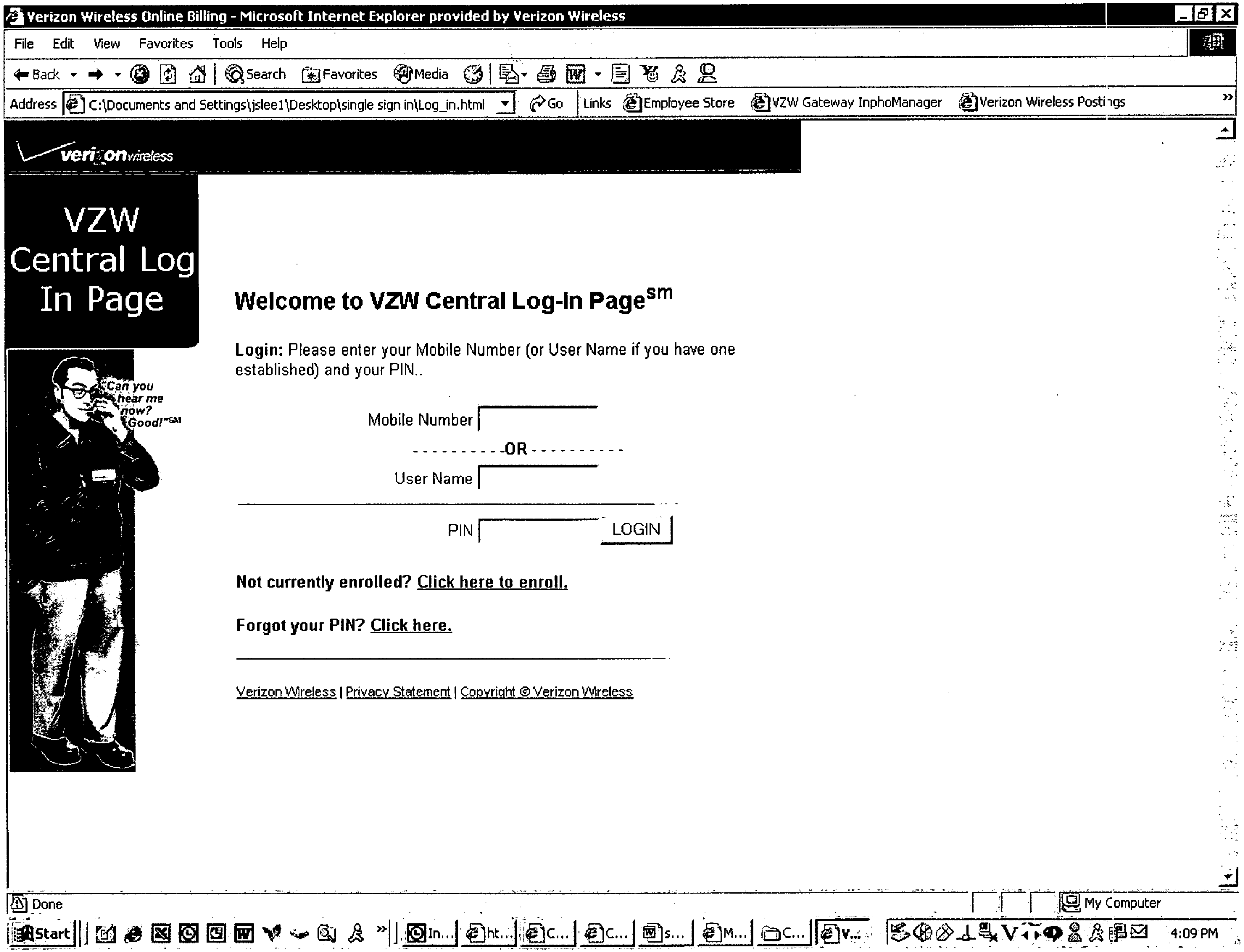
○ Authentication and Single Sign-on of anonymous Web users

- PROBLEM STATEMENT:
  - Product Server needs to authenticate a user logging in for access to profile information stored on the Product Server.
  - Solution should utilize a single username/password among all products, and allow users to click among different product web sites without requiring re-entry of username or password.
  - Products effected: PTT, vtext, Voice Portal, possibly WAP MMS or 802.11 in the future.
- SOLUTION
  - Today – login page and central Oracle database hosted by TCS. HTTP redirects to individual applications
  - Future – utilize capabilities of AAA server and database to store username/password along with current AAA data
  - Required functionality:
    - Support Web interface for user to enter username and password
    - Provide a method for user to manage the password.
    - For a user that does not yet have a Web login password, generate a temporary password and send it to the user in an SMS message.
- STATUS:
  - Current solution is being implemented. Central Oracle database currently in-use for Vtext. HTTP redirects currently used for Vtext alerts. 3-4 week integration and testing each time a product is done. Web design in-process.
  - Future solution is under evaluation.

Solution #3 – Authorization: 2 Levels

- **Basic Authorization**
  - PROBLEM STATEMENT
    - Products need to verify that the user is authorized to use the service.
    - Example products affected: 802.11, 3rd Party Apps.
  - SOLUTION
    - Include product authorization information in the AAA.
    - Products query into the AAA for authorization.
    - Required functionality: AAA returns a yes/no value to Product Server indicating whether the user (based on NAI, MDN, MIN, user name or IP) is authorized to use the service.
  - STATUS: Currently under investigation.

- **Service Type**
  - PROBLEM STATEMENT
    - Product Server or application has predefined service types (i.e. class of service), and needs to know which service type to use (example: Microsoft multiple bundles).
    - Example products affected: 802.11, 3rd Party Apps.
  - SOLUTION
    - Include product authorization information in the AAA.
    - Products query into the AAA for authorization.
    - Required functionality; AAA returns a yes/no value to Product Server indicating whether the user (based on NAI, MDN, MIN, user name or IP) is authorized to use the service.
  - STATUS: Currently under investigation.


Verizon Wireless Online Billing - Microsoft Internet Explorer provided by Verizon Wireless
File Edit View Favorites Tools Help
Back Search Favorites Media
Address C:\Documents and Settings\jslee1\Desktop\single sign in\Log_in.html
Go
Links Employee Store VZW Gateway InphoManager Verizon Wireless Postings
verizon wireless
Can you hear me now? Good!SM
Done
My Computer
Start
In... ht... C... C... s... M... C... v...
4:09 PM

VZW Central Log In Page

Welcome to VZW Central Log-In Page^{sm}

Login: Please enter your Mobile Number (or User Name if you have one established) and your PIN..

Mobile Number

-----------OR-----------

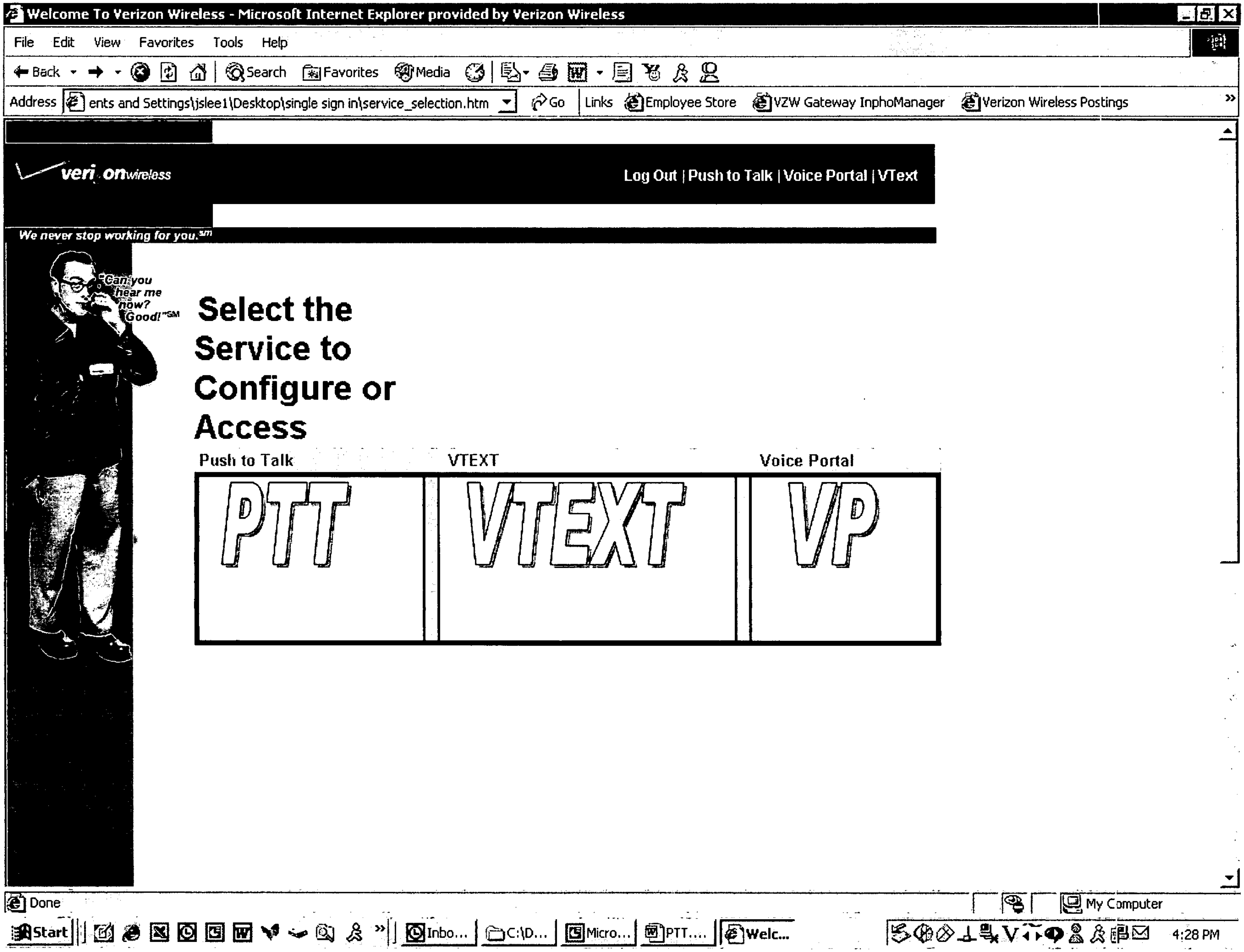
User Name

PIN LOGIN

Not currently enrolled? Click here to enroll.

Forgot your PIN? Click here.

Verizon Wireless | Privacy Statement | Copyright © Verizon Wireless

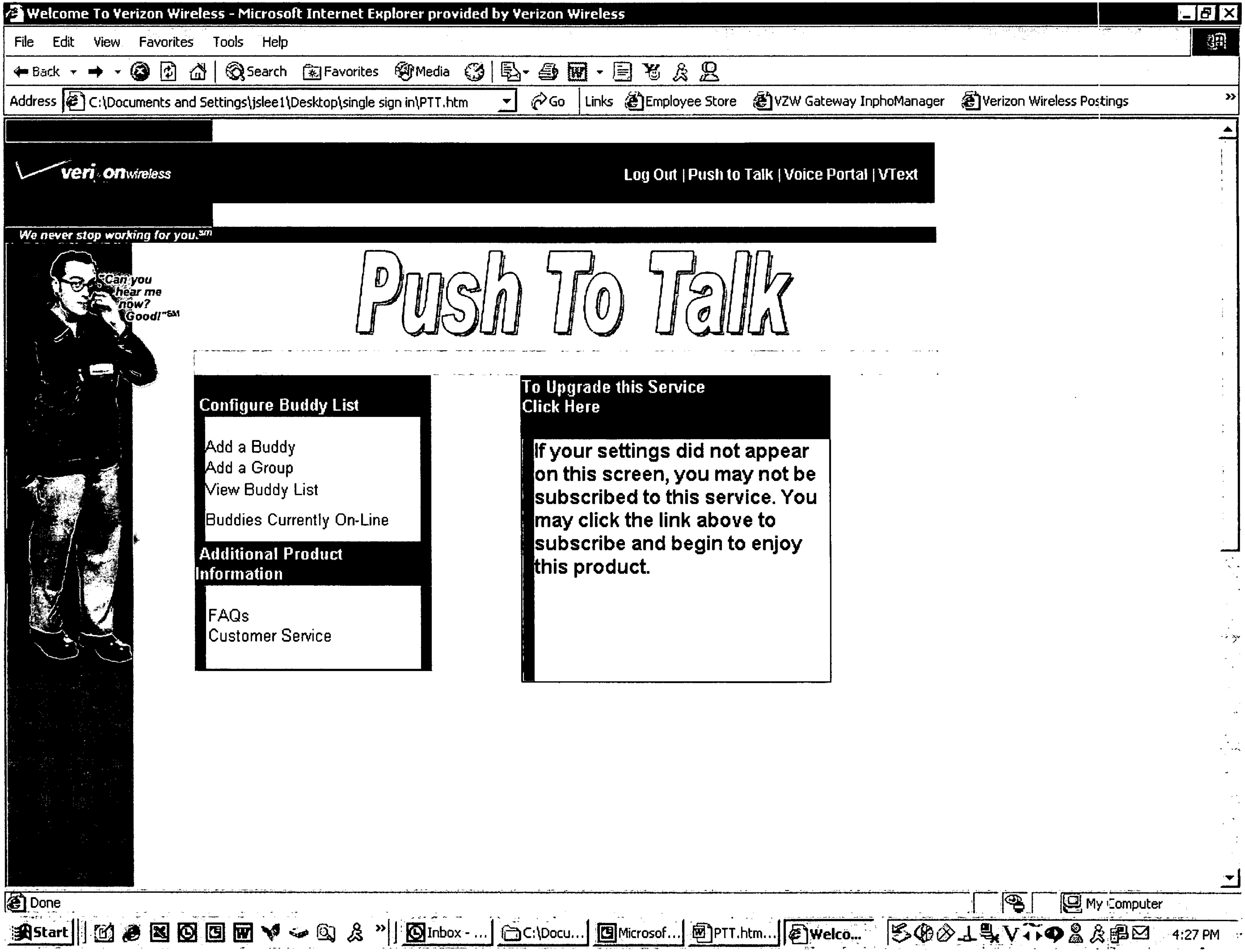


Welcome To Verizon Wireless - Microsoft Internet Explorer provided by Verizon Wireless
File Edit View Favorites Tools Help
Back Search Favorites Media
Address ents and Settings\jslee1\Desktop\single sign in\service_selection.htm
Go
Links Employee Store VZW Gateway InphoManager Verizon Wireless Postings
veri on wireless
Log Out | Push to Talk | Voice Portal | VText
We never stop working for you.SM
"Can you hear me now? Good!"SM

Select the Service to Configure or Access

Push to Talk	VTEXT	Voice Portal
PTT	VTEXT	VP

Done
My Computer
Start
Inbo...
C:\D...
Micro...
PTT....
Welc...
4:28 PM



Welcome To Verizon Wireless - Microsoft Internet Explorer provided by Verizon Wireless
File Edit View Favorites Tools Help
Back Search Favorites Media
Address C:\Documents and Settings\jslee1\Desktop\single sign in\PTT.htm
Go Links Employee Store VZW Gateway InphoManager Verizon Wireless Postings
verizonwireless
Log Out | Push to Talk | Voice Portal | VText
We never stop working for you.℠
Can you hear me now? Good!℠
Done
My Computer
Start Inbox - ... C:\Docu... Microsof... PTT.htm... Welco...
4:27 PM

Push To Talk

Configure Buddy List

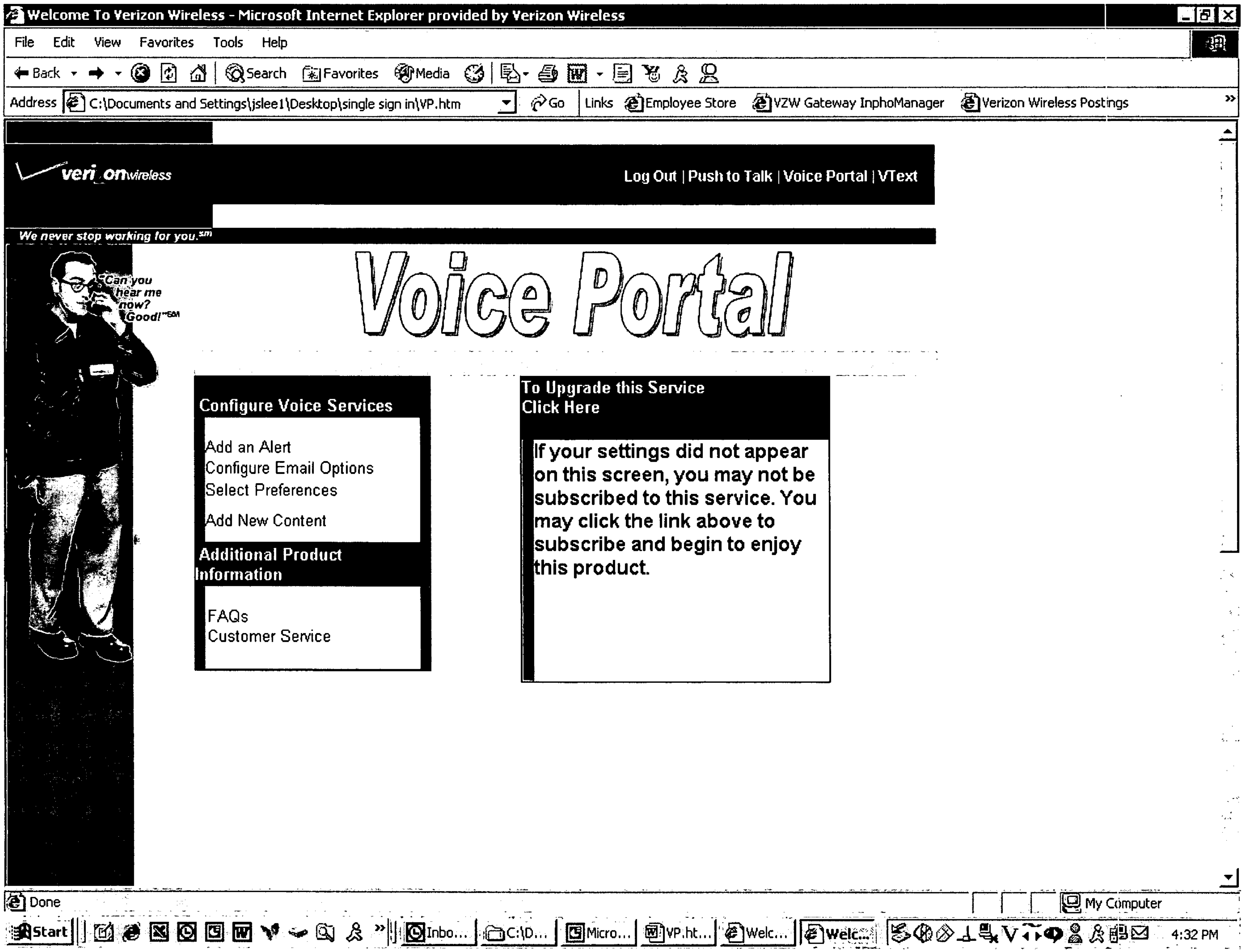
Add a Buddy
Add a Group
View Buddy List
Buddies Currently On-Line

Additional Product Information

FAQs
Customer Service

To Upgrade this Service Click Here

If your settings did not appear on this screen, you may not be subscribed to this service. You may click the link above to subscribe and begin to enjoy this product.


Welcome To Verizon Wireless - Microsoft Internet Explorer provided by Verizon Wireless
File Edit View Favorites Tools Help
Back Search Favorites Media
Address C:\Documents and Settings\jslee1\Desktop\single sign in\VP.htm
Go Links Employee Store VZW Gateway InphoManager Verizon Wireless Postings
veri on wireless
Log Out | Push to Talk | Voice Portal | VText
We never stop working for you.sm
Can you hear me now? Good!™SM
Voice Portal
Done
My Computer
Start
Inbo... C:\D... Micro... VP.ht... Welc... Welc...
4:32 PM

Configure Voice Services

Add an Alert
Configure Email Options
Select Preferences
Add New Content

Additional Product Information

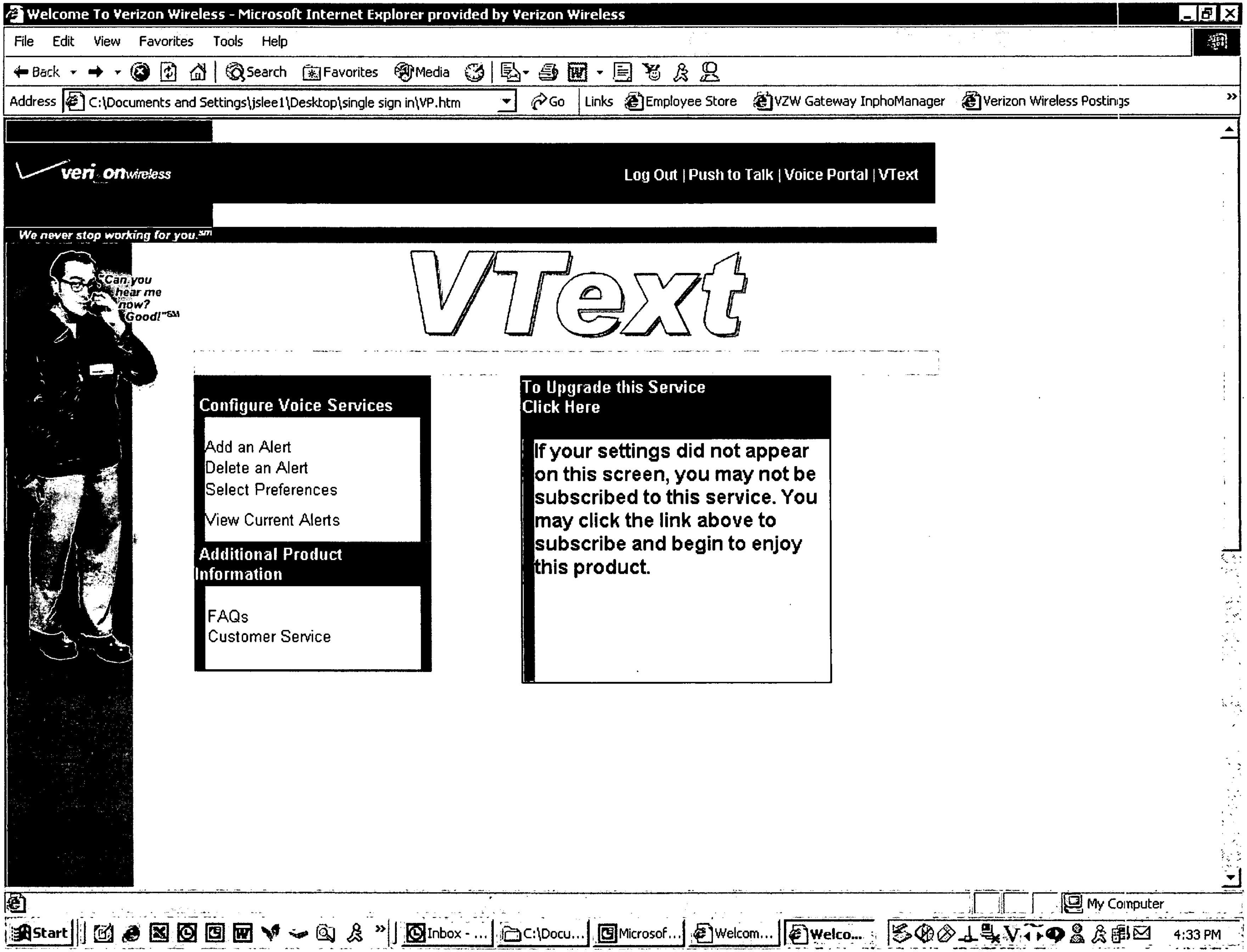
FAQs
Customer Service

To Upgrade this Service
Click Here

If your settings did not appear on this screen, you may not be subscribed to this service. You may click the link above to subscribe and begin to enjoy this product.

RESTRICTED AND PROPRIETARY

The information contained herein is for use by authorized Verizon Wireless employees with a need to know it and should not be disclosed to others.


Welcome To Verizon Wireless - Microsoft Internet Explorer provided by Verizon Wireless
File Edit View Favorites Tools Help
Back Search Favorites Media
Address C:\Documents and Settings\jslee1\Desktop\single sign in\VP.htm Go Links Employee Store VZW Gateway InphoManager Verizon Wireless Postings
verizonwireless
Log Out | Push to Talk | Voice Portal | VText
We never stop working for you.SM
"Can you hear me now? Good!"SM
VText
Start Inbox - ... C:\Docu... Microsof... Welcom... Welco...
My Computer
4:33 PM

Configure Voice Services

Add an Alert
Delete an Alert
Select Preferences
View Current Alerts

Additional Product Information

FAQs
Customer Service

To Upgrade this Service Click Here

If your settings did not appear on this screen, you may not be subscribed to this service. You may click the link above to subscribe and begin to enjoy this product.

Discussion Points – Authentication and Authorization for VZW Products

Overview of What Product Servers and Applications Need

- **Authentication**
  - **Wireless Device:** Product Server needs to verify the identification of a user requesting service from a wireless device. Example products effected: WAP, PTT, MMS.
    - Required functionality: Product Server sends an originator's IP address, received in IP packet, to AAA (session database). AAA (session database) returns trusted MIN (received over R-P interface – authenticated MIN).
  - **Web Access:** Product Server needs to authenticate a user logging in for access to profile information stored on the Product Server. Products effected: PTT, vtext, Voice Portal, possibly WAP MMS or 802.11 in the future.
    - Required functionality:
      - » Support Web interface for user to enter username and password
      - » Provide a method for user to manage the password.
      - » For a user that does not yet have a Web login password, generate a temporary password and send it to the user in an SMS message.

- **Authorization**. Two levels of authorization:
  - **Basic:** Product Server needs to verify that the user is authorized to use the service.
    - Required functionality: AAA returns a yes/no value to Product Server indicating whether the user (based on NAI, MDN, MIN, User ID or IP) is authorized to use the service. Example products affected: 802.11, 3rd Party Apps.
  - **Service Type:** Product Server or application has predefined service types (i.e. class of service), and needs to know which service type to use (example: Microsoft multiple bundles).
    - Required functionality: AAA performs basic authorization as described above, and returns service class or type. Example products affected: MS Multiple Bundles, 3rd Party Apps, and maybe WAP, PTT, and 802.11

Requirements for Individual Applications (See previous page for descriptions)

- **MMS**
  - Authentication
    - Wireless Device – yes (by MIN < -- > IP mapping)
    - Web Access – no (maybe in future)
  - Authorization
    - Basic – yes
    - Service Type – no
      (maybe in future)
- **Push to Talk**
  - Authentication
    - Wireless Device – yes (by MIN < -- > IP mapping)
    - Web Access – yes (for password management and profile access)
  - Authorization
    - Basic - yes
    - Service Type - maybe
- **802.11**
  - Authentication
    - Wireless Device – yes (by NAI from roaming partner)
    - Web Access – yes (for password management only)
  - Authorization
    - Basic - yes
    - Service Type - maybe

Requirements for Individual Applications

- **3rd Party Applications (e.g. MSN Multiple Bundles)**
  - Authentication
    - Wireless Device - no
    - Web Access – no (done through VZW-MSN)
  - Authorization
    - Basic - yes
    - Service Type – yes
- **WAP**
  - Authentication
    - Wireless Device – yes (by MIN < -- > IP mapping)
    - Web Access – not today
  - Authorization
    - Basic - yes
    - Service Type – maybe
- **1X**
  - Authentication
    - Wireless Device – yes (by IS835)
    - Web Access – yes (for password management only)
  - Authorization
    - Basic – yes by IS835
    - Service type - no

Requirements for Centralized Single Sign-on Using AAA Server

verizonwireless

- **Information: The AAA must store the following information to be used for desired functionality**
  - Subscriber Identification Information
    - MIN – provisioned by MTAS
    - MDN – provisioned by MTAS
    - NAI – generated based on provisioned MDN
    - User-ID – chosen by user
  - Authentication Information
    - 1X infrastructure Password – programmed into device (default today is "vzw")
    - User-defined Password – chosen and entered by user
    - Authentication keys for MIP
  - Authorization Information – yes/no field provisioned by MTAS and a service type indicator (when required)
    - Services: 1X, EVDO, 802.11
    - Products: Vtext, PTT, WAP, MMS
    - 3rd Parties: MSN Multiple Bundles
- **Functionality**
  - Queries for authentication.
    - Wireless Device: Product Server sends originator's IP address received in IP packet to AAA (session database). AAA (session database) returns MIN.
    - Web Access
      - Support Web interface for user to enter username and password and manage password
      - For a user that does not yet have a Web login password, generate a temporary password and send it to the user in an SMS message.
  - Queries for authorization information.
    - Basic: Product Server sends IP address, NAI, 802.11, MDN or user ID. AAA returns yes or no to authorize.
    - Service Type: Product Server sends IP address, NAI, 802.11, MDN or user ID. AAA returns a service type indicator.

Web-Based Password Management

verizonwireless

- **Currently, vtext.com has a web-based user ID, password management system.**
- **Two options:**
  - Option 1 – TCS front-end, AAA data store
    - Expand vtext.com method to include all products and 802.11.
    - Develop a process where storage of user ID password is removed from vtext.com. The web interface will store the user ID password in the AAA data store.
  - Option 2 – AAA front-end, AAA data store
    - Eliminate vtext.com user ID password method and database.
    - Develop user ID password process for AAA.

Invention Disclosure

Please fill out the Invention Disclosure Form as completely as possible. This form must be approved by business group management, executive director or director. If you have any questions about the form, or about your invention, please contact Invention Administration Office at (908) 607-8141 or e-mail invention@verizonwireless.com. Please return the form, signed by each inventor, and witnessed, with drawings and flow charts (software inventions or processes) as appropriate to:

Verizon Wireless
Technology Development Department
Headquarters, Satellite Office
30 Independence Blvd
Warren, NJ 07059
Attn: Invention Administration Office

veri onwireless

Invention Disclosure

Do Not Write in This Area

Docket No. ______

Business Group ______

Attorney ______

Disposition ______

Title of Invention Authentication / Single Sign On

Inventor 1 Varsha Clare
Full Name Including Middle Name
Work Phone 925-279-6038
E-mail Address Varsha.clare@verizonwireless.com
Citizenship US
Home Address 984 Gray Fox Circle, Pleasanton, CA 94566
Number and Street, City, State, ZIP Code, Country or Province

Inventor 2 Allen Billings
Full Name Including Middle Name
Work Phone 925-279-6592
E-mail Address Allen.billings@verizonwireless.com
Citizenship US
Home Address 8 Bernice #108, San Francisco, CA 94103
Number and Street, City, State, ZIP Code, Country or Province

Inventor 3 Kent W. Hughes
Full Name Including Middle Name
Work Phone 925-279-6511
E-mail Address Kent.Hughes@verizonwireless.com
Citizenship US
Home Address 5830 Ivanhoe Road, Oakland, CA 94618
Number and Street, City, State, ZIP Code, Country or Province

Inventor 4 ______
Full Name Including Middle Name
Work Phone ______
E-mail Address ______
Citizenship ______
Home Address ______
Number and Street, City, State, ZIP Code, Country or Province

Date First Made Invention (Conception Date) [redacted]

Engineering Reports, etc. ______ **Pages** ______ **Date** ______

Journals, Conference Proceedings ______ **Date** ______

Has the invention been disclosed outside Verizon Wireless? ☒ Yes □ No **Date** ______

Has the invention been demonstrated? □ Yes ☒ No **Date** ______

Has a product using the invention been shipped outside Verizon Wireless? □ Yes ☒ No **Date** ______

Was work done under a government contract? □ Yes ☒ No **No.** ______

Who is responsible for this (these) contract(s)? ______ **Phone No.** ______

COMMERCIAL FACTORS

Is the device or process now in production or used commercially? □ Yes ☒ No

If so, date first used ______ **Date product first sold** ______ **Model Number** ______

If not, is use or production being considered? ______ **When?** ______

To which of Verizon Wireless's business or telephone operating companies would this invention be of Network

interest?

What Verizon Wireless competitors are most likely to use this invention? Wireless and wireline operators.

How would use by a competitor be discovered? Published information, direct use of service by our staff.

The information requested below may serve as the basis for a patent application, therefore be as complete and as accurate as possible. Please describe your invention on added pages to be attached hereto using the following outline as a guide.

1. **Abstract of the Invention** — In a few sentences, briefly describe what your invention is and what it does.

   This is a standardized process for: 1) Authentication of subscriber using services such as MMS, PTT; 2) Authorization of various service use by a subscriber, e.g., 802.11; 3) Single sign on user id, password for various services, e.g., MMS, PTT, vtext.com and automatic process of sending user id, password to applications platforms.

2. **Background Information** — Provide sufficient background information so that the function and novelty of your invention can be understood. What techniques prior to your invention were used to perform the function of your invention, and what are the disadvantages? What problem is solved by your invention? What are the advantages of your invention over the prior techniques?
   1. Without proper authentication, there is a possibility that MIN/MDN delivered by the client (in handset) may be altered before reaching the application platform
   2. Without single user id, password, VZW subscriber will be forced to set up and manage multiple user ids and passwords. VZW applications will need to develop user id, password in each application.

3. **Detailed Description** — (a) Describe the structural *and* functional operation of your invention. Use drawings, graphs, or flowcharts as needed to describe your invention. Give specific details, not just general information. Point out what improvements your invention incorporates or the superior performance which is obtained and *why* it is obtained. (b) Are there any alternative methods or different structural embodiments of your invention? Can the general idea or technique of your invention be extended to other related fields? (c) Which features are believed to be the novel features (be specific)?

   Attached Documents:
   1. **Sign On Requirements v2.0[redacted]**
   2. **Data Product Authentication Briefing v2.2[redacted]**

4. **Attach a copy of the most pertinent publications to your invention that are known to you.**

5. **After the disclosure is prepared, the inventors MUST sign in the spaces below. The witnesses should read and understand the disclosure and sign in the appropriate spaces below. The inventors and witnesses should initial and date each added page of disclosure.**

Inventor Varsha Clare **Date** ____________

Inventor Allen Billings **Date** ____________

Inventor Kent Hughes **Date** ____________

Inventor ____________ **Date** ____________

Witnessed and Understood By ____________ **Date** ____________

Witnessed and Understood By ____________ **Date** ____________

Prepared By ______________________________ Date ____________

Business Group Name ______________________________

Executive Director Approval ______________________________ Date ____________

GUIDELINES FOR INVENTION DISCLOSURES

A detailed explanation of the Invention Disclosure Form follows:

TITLE OF INVENTION

The title should be brief and descriptive. More often than not, it will change during the drafting of the patent application.

INVENTORS

This includes all persons who may be inventors. By law, the true inventors must be named. It is the patent attorney's responsibility to determine proper inventorship, which is a legal determination. The order of names on a patent has no legal significance.

DATE FIRST MADE INVENTION

Conception Date

This item has legal significance and should be carefully considered. Conception is the mental formulation of a complete idea for a product or process including a means of practicing the invention and a utility. To have a complete conception of a new product, it is necessary to provide the product, a method of preparing the product (unless such method would be obvious) and a utility for the product (unless such utility would be obvious).

First Disclosure to Others

This item can also have significant legal consequences. If there has been any disclosure outside the company, the date of any non-disclosure agreement or other relevant agreement should be indicated.

COMMERCIAL FACTORS

Include any agreements with consultants or other companies which may be relevant to the invention. Any expected or contemplated sale, offer for sale, commercial use or third party disclosure of the invention must be reported to the Legal Department.

ABSTRACT OF THE INVENTION

This is basically intended to be a summary. Any useful background information should be provided.

BACKGROUND INFORMATION

List the relevant prior art retrieved in the prior art search. Inventors have an uncompromising duty of candor to the U.S. Patent Office. Thus, if there is any question whether a document is rdevant, be sure to include it in the list of prior art. In addition, inventors have a continuing duty to bring prior art to the attention of the U.S. Patent Office after filing the patent application. The closest prior art should be clearly distinguishedfrom the invention. Be sure to discuss any of your relevant pending patent applications when you consider the prior art.

DETAILED DESCRIPTION

This is the main section of the disclosure in which the details of the invention are provided. It is intended to provide sufficient information so that the patent attorney understands the full scope of the invention and can begin to draft an appropriate patent application providing the maximum protection possible. Points which should be addressed and questions to consider in this section are listed below. Attachments are generally used to provide the necessary information in sufficient detail.

(a) **Type of Invention:**

What is the invention? Is it a new device, a new or improved process, a new use of an old device, etc. a new design, etc. Show drawings, graphs, or flowcharts to help describe the invention.

(b) **Utility:**

Describe how to use the invention. What is all the possible practical utilities?

(c) **Unobviousness:**

What problems in the prior art are solved by the invention? Would the prior art direct an investigator away from your invention? Give any references which are contradictory to your results. Mention any proposed solutions tried by you or others which failed. Are there surprising or unexpected results or properties of your process or device?

(d) **Variations and Limitations:**

Discuss any variations, modifications, substitutions, or other changes that may be made within the scope of the invention. The invention should be first described in the broadest generic scope contemplated (and permitted by the prior art) and then described in terms of more preferred and most preferred way.

(e) **Explanations:**

Set forth any explanations or theories you may have about how or why your invention functions. Although you may not know exactly why your invention functions and the patent need not contain such information, the information may be helpful to the attorney, particularly when addressing the obviousness of the invention.

SIGNATURES/APPROVALS

After the Invention Disclosure has been signed and dated by all suggested inventors, and witnessed, it should be approved by an inventor's Department Head. It is the Department Head's responsibility to approve the Invention Disclosure form as being complete in terms of (a) description, (b) value to the company and (c) names of all suggested inventors. The Invention Disclosure form is then sent to Invention Administration Office for review. The Invention Disclosure will be evaluated for filing and prioritized, taking into consideration other priorities and recommendations of management.

Single Sign-on
Third-Party Authorization
Vendor and Platform Recommendation

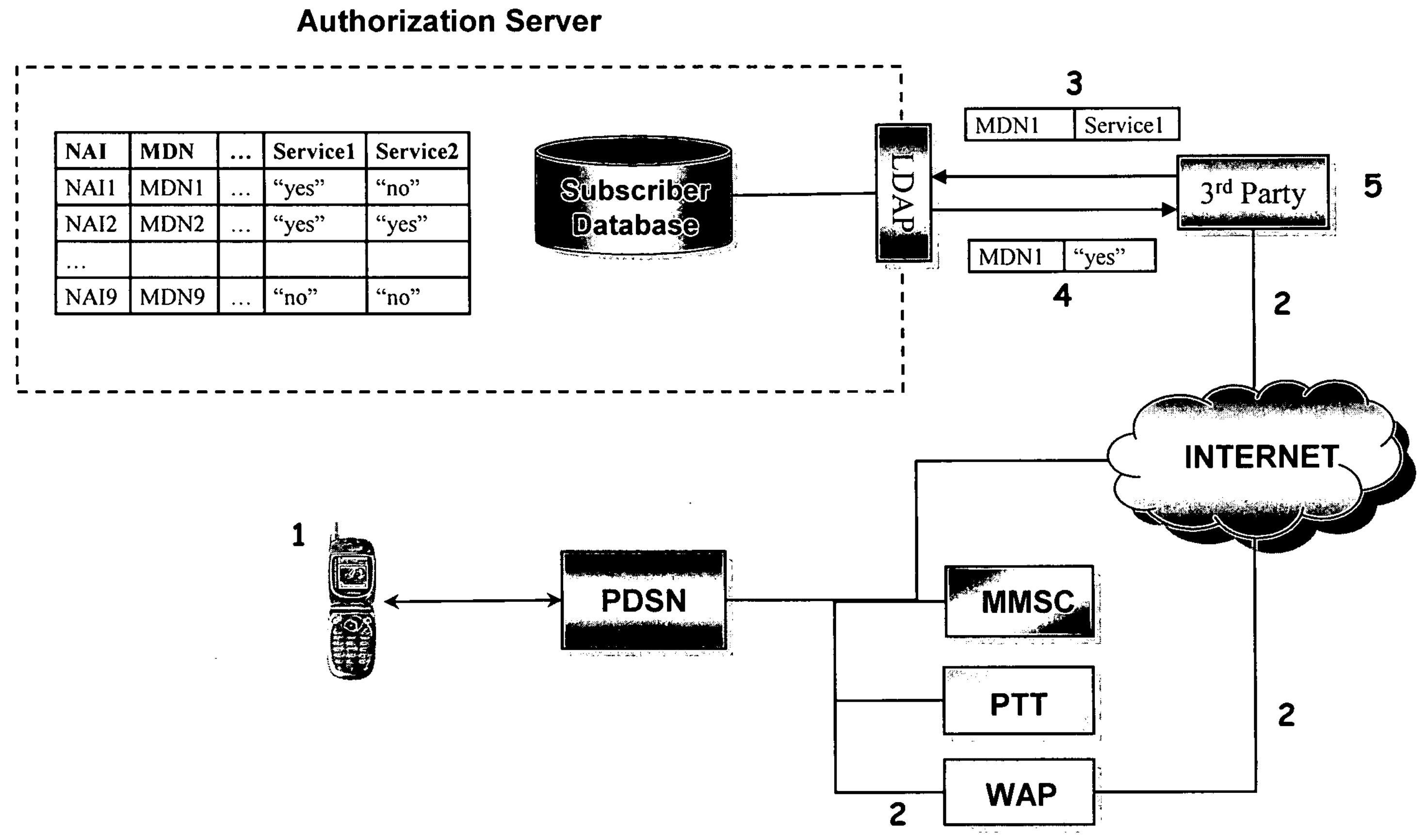
Network Technology Development
Draft Version 1.4
May 7, 2003

RESTRICTED AND PROPRIETARY
The information contained herein is for use by authorized Verizon Wireless & subsidiaries employees with a need to know it and should not be disclosed to others.

Objectives and Requirements

- Objective
  - Allow VZW network elements and 3rd party partners to query an "Authorization Server" for selected information to authorize the use of applications and/or tiers of service per subscriber.
  - Support username/password authentication to extend VZW Single Sign-on functionality to 3rd Parties
  - Since all possible use cases have not been identified, solution should provide flexibility so that the information in the Authorization Server and associated information at the 3rd party or VZW platform can be represented differently.
- Overview of Requirements (see "*SSO - 3rd Party Authorization Requirements v1.1.doc*" for details)
  - Authorization Server must support the ability to create service definitions associated with different applications. A service will contain alpha-numeric or integer fields that can be queried by an application platform or 3rd party provider
  - Information within the service profiles will be accessed through a well-defined, standards-based query (such as LDAP)
    - Query will include the identity of the requestor (platform or 3rd party), the identity of the subscriber (MIN or MDN), the name of the requested field or service, and the user's password if authentication is required
    - Response will include the value of the field(s), MIN, MDN, and the authentication result (yes/no)
  - New service definitions or fields can be added without further development or modification to the query format
  - Authorization Server will provide a secure method to identify a 3rd Party to determine whether the 3rd party is allowed to receive the requested information
- Example Use Cases
  - A 3rd party application provider of WAP services queries the Authorization Server to determine which applications the subscriber is allowed to access (pages 3 and 4)
  - BREW: Users are provisioned for BREW on the Authentication Server. BREW ADS queries Authorization Server to for authorization (page 5)

WAP Example – Query for Specific Services (Using LDAP)

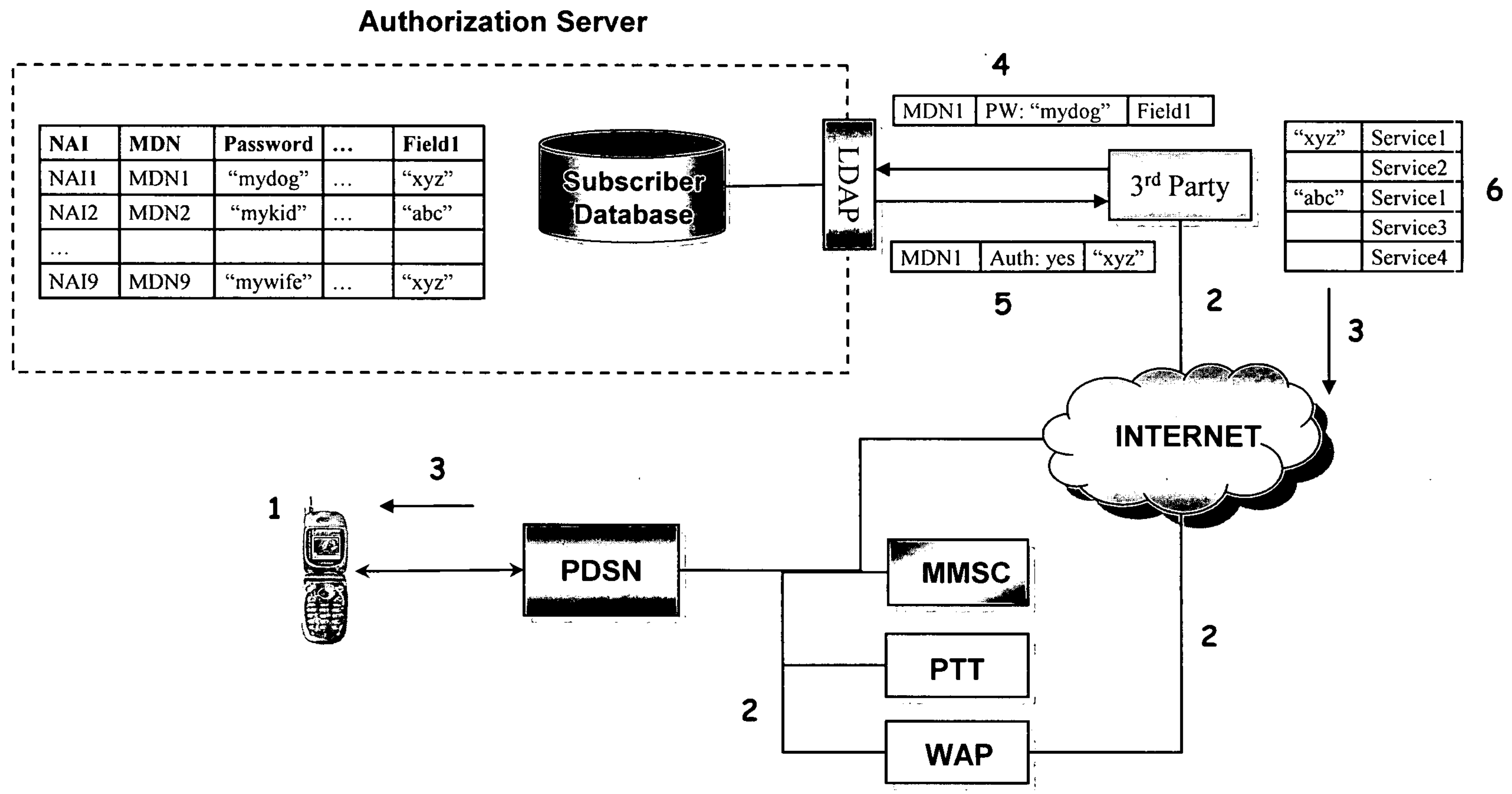


NAI	MDN	…	Service1	Service2
NAI1	MDN1	…	"yes"	"no"
NAI2	MDN2	…	"yes"	"yes"
…				
NAI9	MDN9	…	"no"	"no"

1. User launches WAP browser
2. User is directed by WAP gateway, through the Internet to the 3rd party platform
3. 3rd party queries LDAP interface with MDN and requested service
4. Authorization Server returns yes/no value of service field
5. Access to application is allowed or denied by 3rd Party

RESTRICTED AND PROPRIETARY
The information contained herein is for use by authorized Verizon Wireless employees with a need to know it and should not be disclosed to others.

WAP Example – Query for Service Level With Authentication



NAI	MDN	Password	...	Field1
NAI1	MDN1	"mydog"	...	"xyz"
NAI2	MDN2	"mykid"	...	"abc"
...				
NAI9	MDN9	"mywife"	...	"xyz"

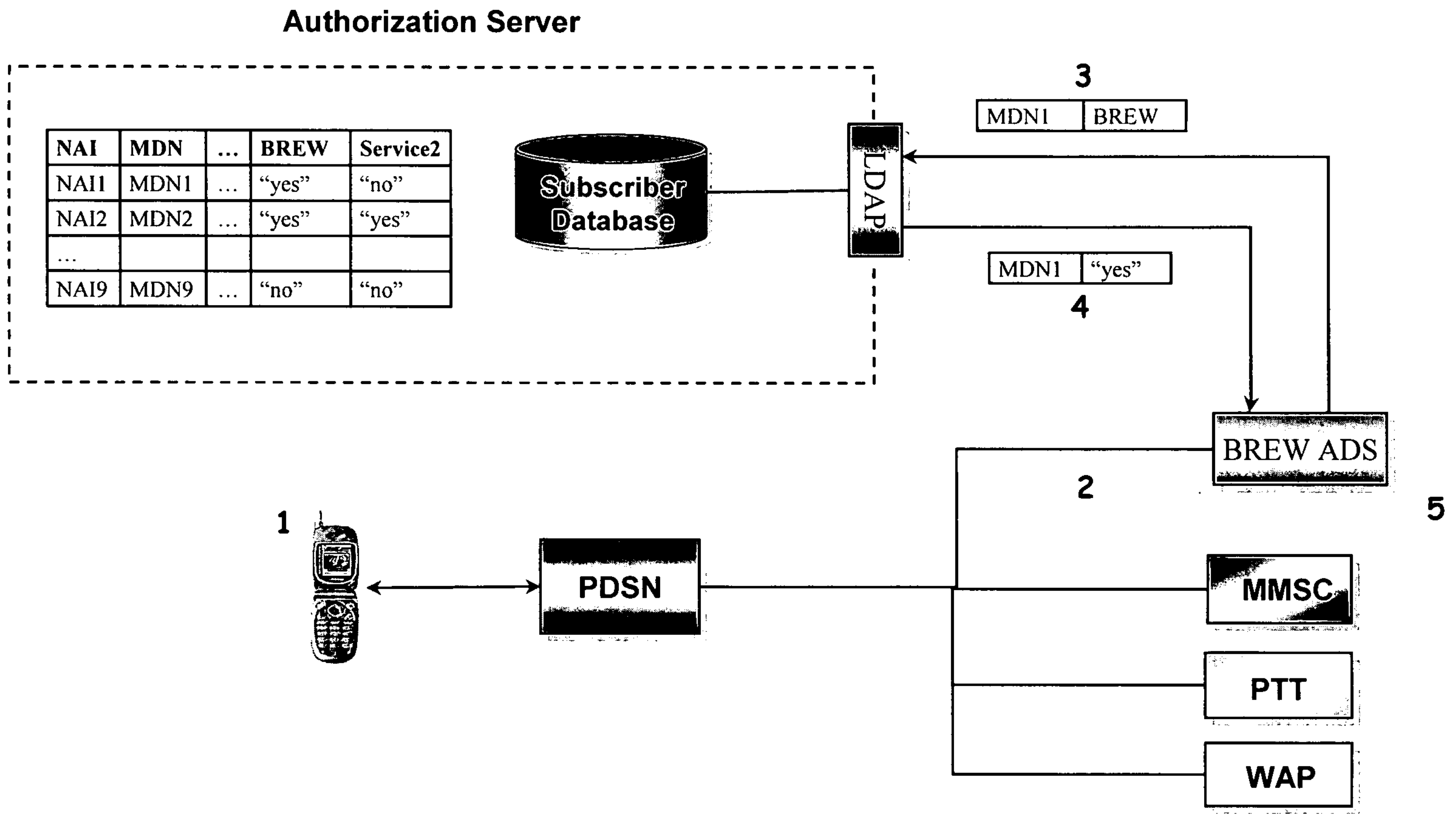
MDN1	PW: "mydog"	Field1

MDN1	Auth: yes	"xyz"

"xyz"	Service1
	Service2
"abc"	Service1
	Service3
	Service4

1. User launches WAP browser
2. User is directed by WAP gateway, through the Internet to the 3rd party platform
3. 3rd party prompts user for username (MDN) and password
4. 3rd party queries LDAP interface with username MDN, password, and requested field with identifier
5. Authorization Server checks username and password and returns identifier to indicate which services are allowed
6. 3rd Party correlates identifier to appropriate service level, and associated services allowed

Authorization for BREW



NAI	MDN	...	BREW	Service2
NAI1	MDN1	...	"yes"	"no"
NAI2	MDN2	...	"yes"	"yes"
...				
NAI9	MDN9	...	"no"	"no"

1. User launches BREW
2. User is directed to BREW ADS
3. ADS queries LDAP interface with MDN and requested service ("BREW")
4. Authorization Server returns yes/no value of service field
5. Access to BREW is allowed or denied

SINGLE SIGN-ON
THIRD PARTY AUTHORIZATION REQUIREMENTS
VERSION 1.2 DRAFT

Issued: May 21, 2003

Confidential and Proprietary Information of Verizon Wireless

Prepared For:

Prepared By:

Technology Development
Verizon Wireless

Document Control

REVISION	ISSUED DATE	DESCRIPTION
Version 1.0	[redacted]	Originally created by Allen Billings
Version 1.1	[redacted]	Incorporated input from Jeff Lee. Added "Provisioning of Service Definitions" and "Sizing" sections.
Version 1.2	May 21, 2003	Added support for user-authentication based on user-defined password.

INTRODUCTION

This document describes the Verizon Wireless (VZW) requirements to deliver Third Party Authorization capability on a server (generically referred to as Authorization Server) installed on the VZW data network. Third Party Authorization will allow VZW applications and third party partners to query the Authorization Server for selected information, which will be used to authorize the use of applications or tiers of service for individual subscribers.

For questions on the content provided in this document please contact Allen Billings at allen.billings@VerizonWireless.com (925) 279-6592.

REQUIREMENTS

1.1 STORAGE AND CONFIGURATION OF SERVICE AUTHORIZATION INFORMATION

The Authorization Server shall store subscriber identification information and service authorization information for each individual subscriber provisioned in the server. At a minimum, the subscriber identification information shall include the user's MIN and MDN, which will be provisioned by VZW, and a user-defined password, which will be populated through a password management interface. At a minimum, the service authorization information shall include an alphanumeric, integer, or Boolean value for each service that VZW chooses to assign. There shall be no hard limit to the number of services associated with a subscriber.

The detailed format of the data must allow for flexibility in defining service authorization information and provisioning API. A final design decision on this format should be jointly made between the Authorization Server vendor and VZW, based largely on the response time and maintenance requirements for each option.

1.2 PROVISIONING OF SERVICE DEFINITIONS

The Authorization Server shall allow different VZW internal users to read, add, modify, and remove service definitions through a convenient user-interface. This interface must have multiple levels of security and user roles. Some VZW users must only be able to read the data while others may add, delete, update, and read.

1.3 USER PROVISIONING

A VZW-customized API shall be provided to allow VZW to add, modify, and remove subscriber records and subscriber services on the Authorization Server. The Authorization Server vendor shall work with VZW to define the provisioning API.

1.4 QUERIES FOR AUTHORIZATION INFORMATION

The Authorization Server shall support secure queries from specified VZW or third party product servers. Queries from product servers will include the identity of the requestor, identity of the subscriber (MIN or MDN), and the names of the requested service authorization fields or parameters. A password may be included if user-authentication is required. The Authorization Server will send a query response to the product server, which will include MIN, MDN, user-authentication result, and the values of the requested service authorization fields or parameters. Additionally, the Authorization Server shall support queries from specified product servers that will return the values of ALL service authorization fields or parameters. The queries and responses shall be based on an industry standard format (For example a subset of current LDAP specifications). The Authorization Server vendor shall supply a detailed technical specification outlining the format of the queries and responses, and all connection and configuration information required to support the authorization queries. This specification shall be provided to any VZW vendor or partner.

1.5 Product Server Authentication, Configuration, and Rights

The Authorization Server shall support a method to securely authenticate specified VZW or third party product servers. The Authorization Server will store configuration information for each individual product server, which will include, as a minimum, a list of the authorization fields or parameters that the product server is allowed to query. Each individual product server must only be allowed to query for authorization fields or parameters specified in its configuration list. The Authorization Server shall allow VZW to add, modify, and remove allowed product server configurations through a convenient user-interface.

1.6 Sizing

The Authorization Server shall be configured with adequate storage capacity to store authorization information for the entire VZW subscriber base of roughly 31 million. A subset of this subscriber base will be considered active users for the purpose of traffic calculations. A traffic model will be created to determine the transaction rate that must be supported.

REQUIREMENTS SIGNATORIES

Cellco Partnership d/b/a Verizon Wireless

By: ____

Title: ____

< Vendor >

By: ____

Title: ____

Verizon Wireless
Product Authentication Project Plan
6/2/2003

Activity	Owner	Due Date	Completed Date	Notes
Load software into staging	Thomas May	6/6/2003		** Originally scheduled 5/30 - postponed due to other AAA priorities - no impact to LDAP products
Load software into production	Thomas May	7/11/2003		** Originally scheduled 6/20 - postponed due to other AAA priorities - no impact to LDAP products
MMS - complete development testing *	Xuming Chen	6/13/2003		
MMS - begin testing in staging	Xuming Chen	6/20/2003		
MMS - end testing in staging	Xuming Chen	6/27/2003		
MMS - begin testing in production	Xuming Chen	7/30/2003		
MMS - end testing in production	Xuming Chen	8/6/2003		
MMS - LDAP network ready	Xuming Chen	8/6/2003		
WAP2 - complete development testing *	Jude Munn	7/14/2003		
WAP2 - begin testing in staging	Jude Munn	7/21/2003		
WAP2 - end testing in staging	Jude Munn	7/28/2003		
WAP2 - begin testing in production	Jude Munn	8/18/2003		
WAP2 - end testing in production	Jude Munn	8/25/2003		
WAP2 - LDAP network ready	Jude Munn	8/25/2003		
PTT - complete development testing *	Ian DeCone	TBD		
PTT - begin testing in staging	Ian DeCone	TBD		
PTT - end testing in staging	Ian DeCone	TBD		
PTT - begin testing in production	Ian DeCone	TBD		
PTT - end testing in production	Ian DeCone	TBD		
PTT - network ready	Ian DeCone	TBD		
* Pass Bridgewater criteria				

Product Authentication (LDAP) Architecture for Alarming Scenarios

DRAFT

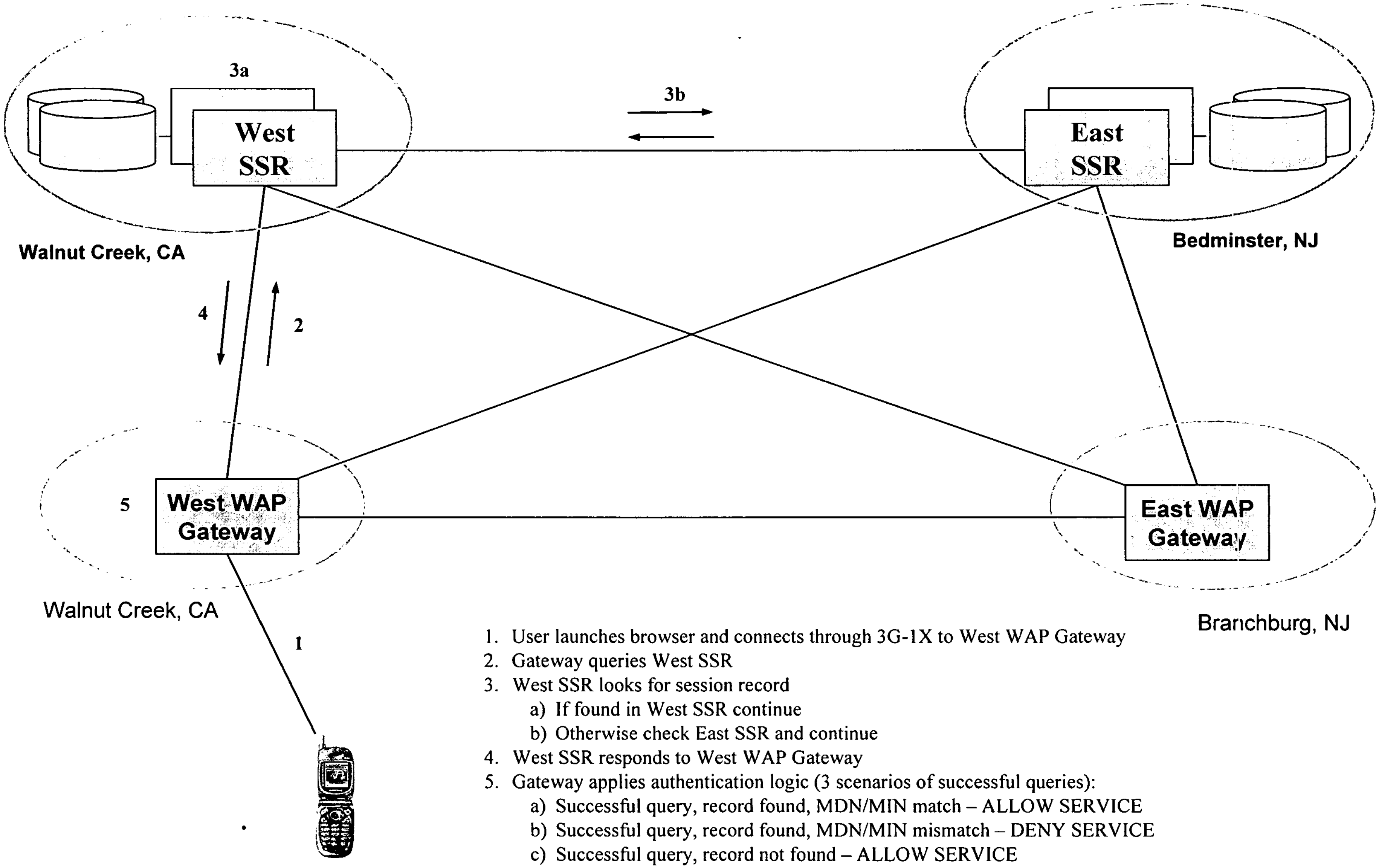
Network Technology Development

Allen Billings, Jude Munn

Draft Version 1.0
June 20, 2003

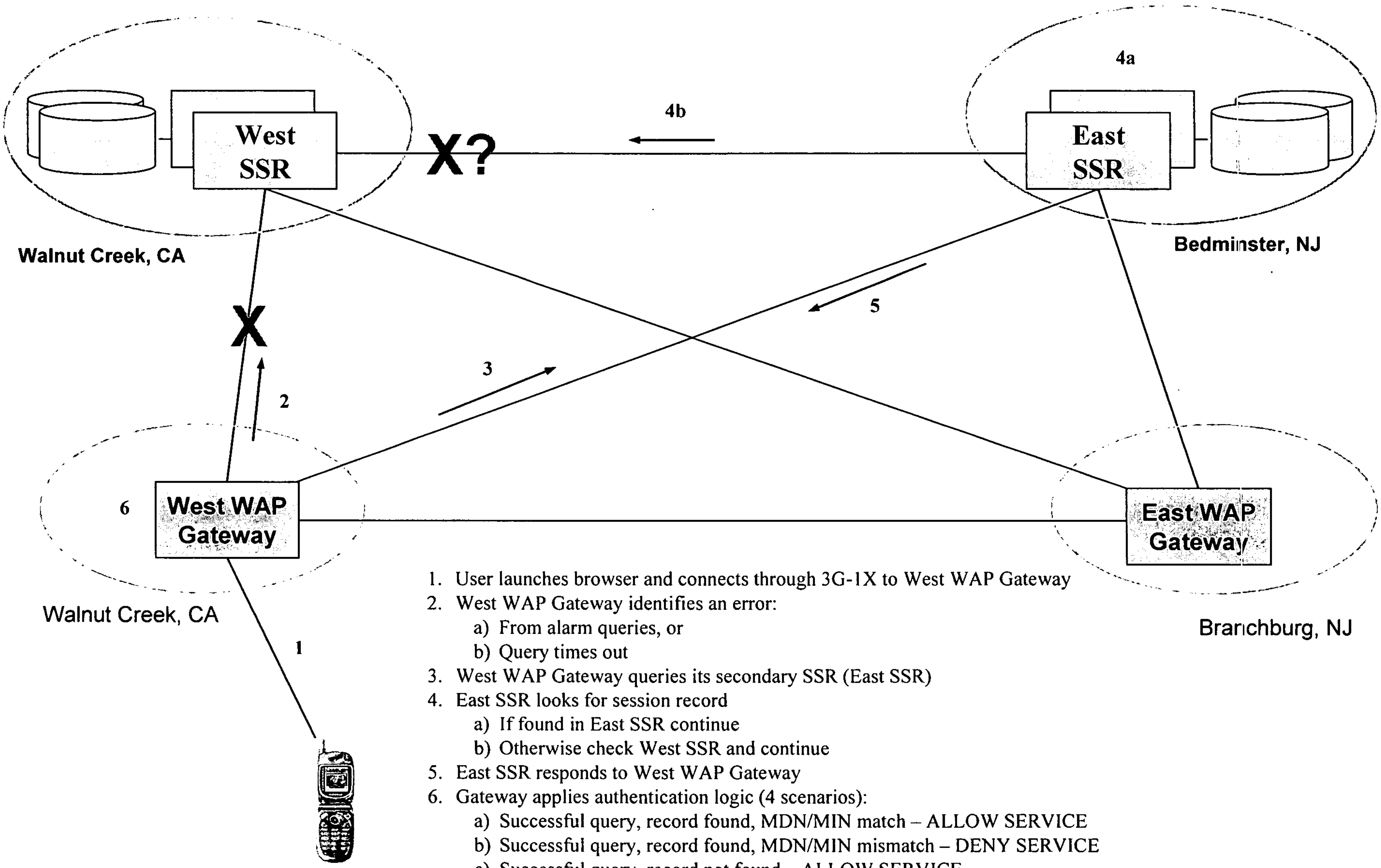
RESTRICTED AND PROPRIETARY
The information contained herein is for use by authorized Verizon Wireless & subsidiaries employees with a need to know it and should not be disclosed to others.

Customer Connection – Successful LDAP Query



1. User launches browser and connects through 3G-1X to West WAP Gateway
2. Gateway queries West SSR
3. West SSR looks for session record
   a) If found in West SSR continue
   b) Otherwise check East SSR and continue
4. West SSR responds to West WAP Gateway
5. Gateway applies authentication logic (3 scenarios of successful queries):
   a) Successful query, record found, MDN/MIN match – ALLOW SERVICE
   b) Successful query, record found, MDN/MIN mismatch – DENY SERVICE
   c) Successful query, record not found – ALLOW SERVICE

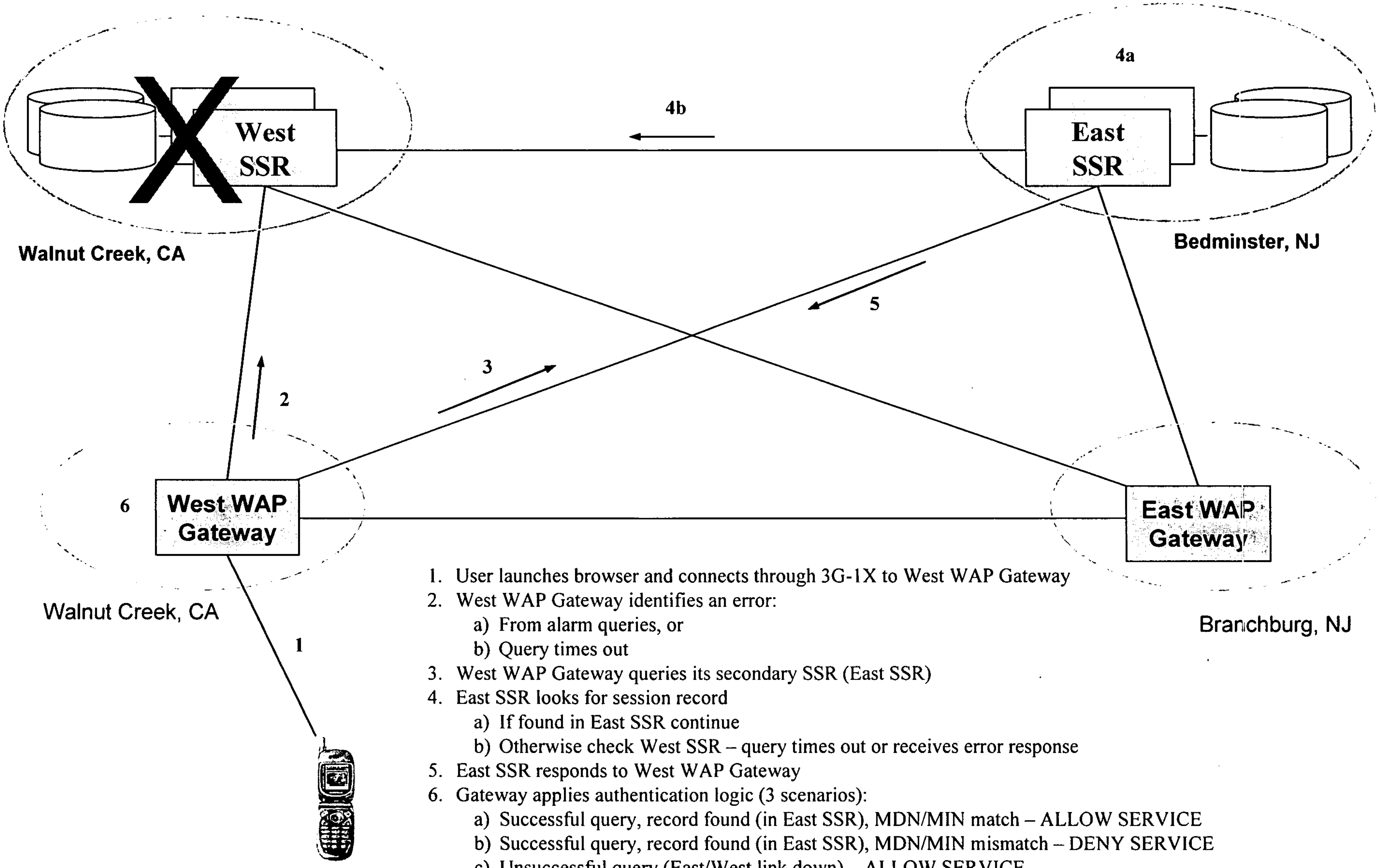
Customer Connection – Link Down



1. User launches browser and connects through 3G-1X to West WAP Gateway
2. West WAP Gateway identifies an error:
    a) From alarm queries, or
    b) Query times out
3. West WAP Gateway queries its secondary SSR (East SSR)
4. East SSR looks for session record
    a) If found in East SSR continue
    b) Otherwise check West SSR and continue
5. East SSR responds to West WAP Gateway
6. Gateway applies authentication logic (4 scenarios):
    a) Successful query, record found, MDN/MIN match – ALLOW SERVICE
    b) Successful query, record found, MDN/MIN mismatch – DENY SERVICE
    c) Successful query, record not found – ALLOW SERVICE
    d) Unsuccessful query (East/West link down) – ALLOW SERVICE

RESTRICTED AND PROPRIETARY
The information contained herein is for use by authorized Verizon Wireless employees with a need to know it and should not be disclosed to others.

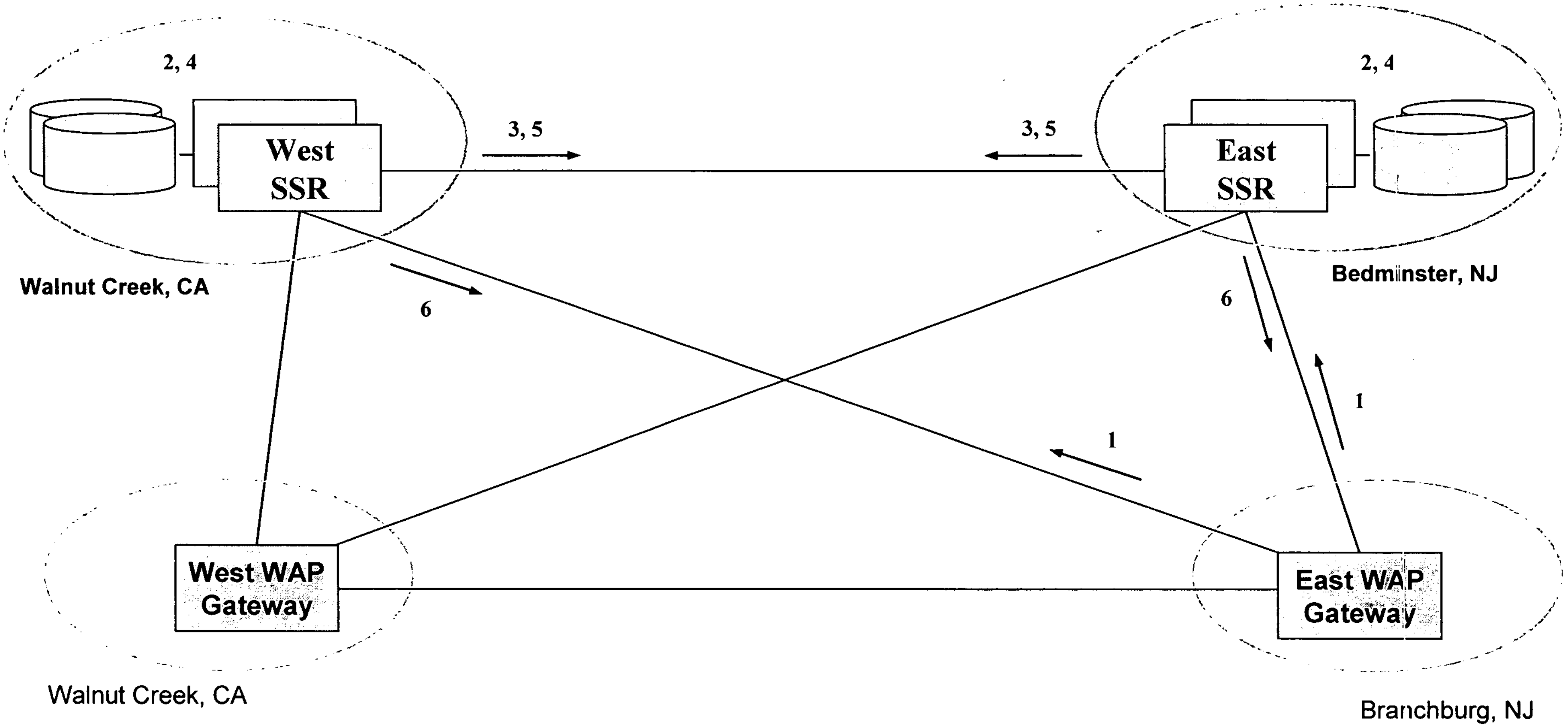
Customer Connection – SSR Down



1. User launches browser and connects through 3G-1X to West WAP Gateway
2. West WAP Gateway identifies an error:
   a) From alarm queries, or
   b) Query times out
3. West WAP Gateway queries its secondary SSR (East SSR)
4. East SSR looks for session record
   a) If found in East SSR continue
   b) Otherwise check West SSR – query times out or receives error response
5. East SSR responds to West WAP Gateway
6. Gateway applies authentication logic (3 scenarios):
   a) Successful query, record found (in East SSR), MDN/MIN match – ALLOW SERVICE
   b) Successful query, record found (in East SSR), MDN/MIN mismatch – DENY SERVICE
   c) Unsuccessful query (East/West link down) – ALLOW SERVICE

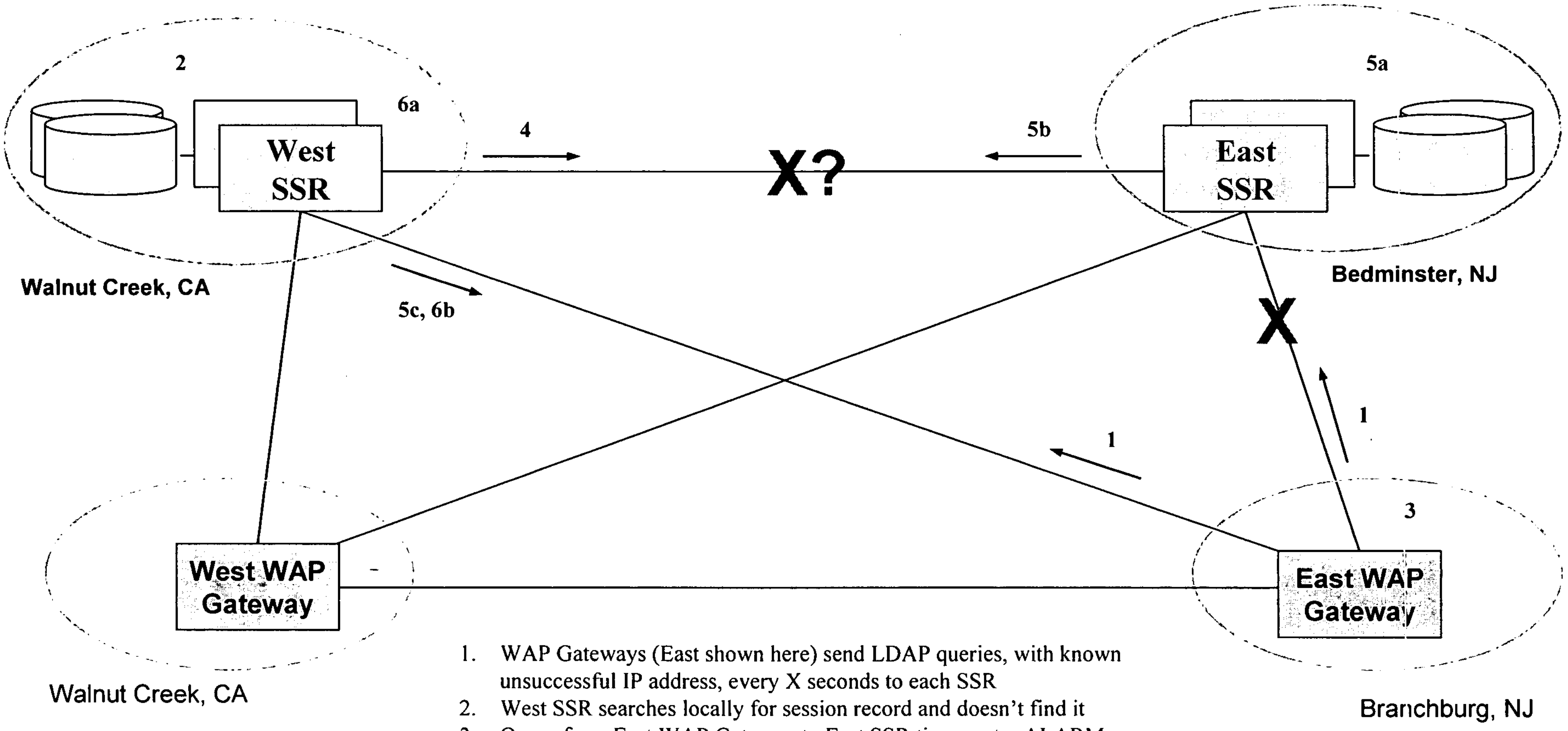
RESTRICTED AND PROPRIETARY
The information contained herein is for use by authorized Verizon Wireless employees with a need to know it and should not be disclosed to others.

Alarming Queries – Successful Response



1. WAP Gateways (East shown here) send LDAP queries, with known unsuccessful IP address, every X seconds to each SSR
2. Each SSR searches locally for session record and doesn't find it
3. Original SSR passes query to remote SSR
4. Remote SSR searches for session record and doesn't find it
5. Remote SSR returns null response
6. Original SSR returns null response to WAP Gateway - CONFIRMED

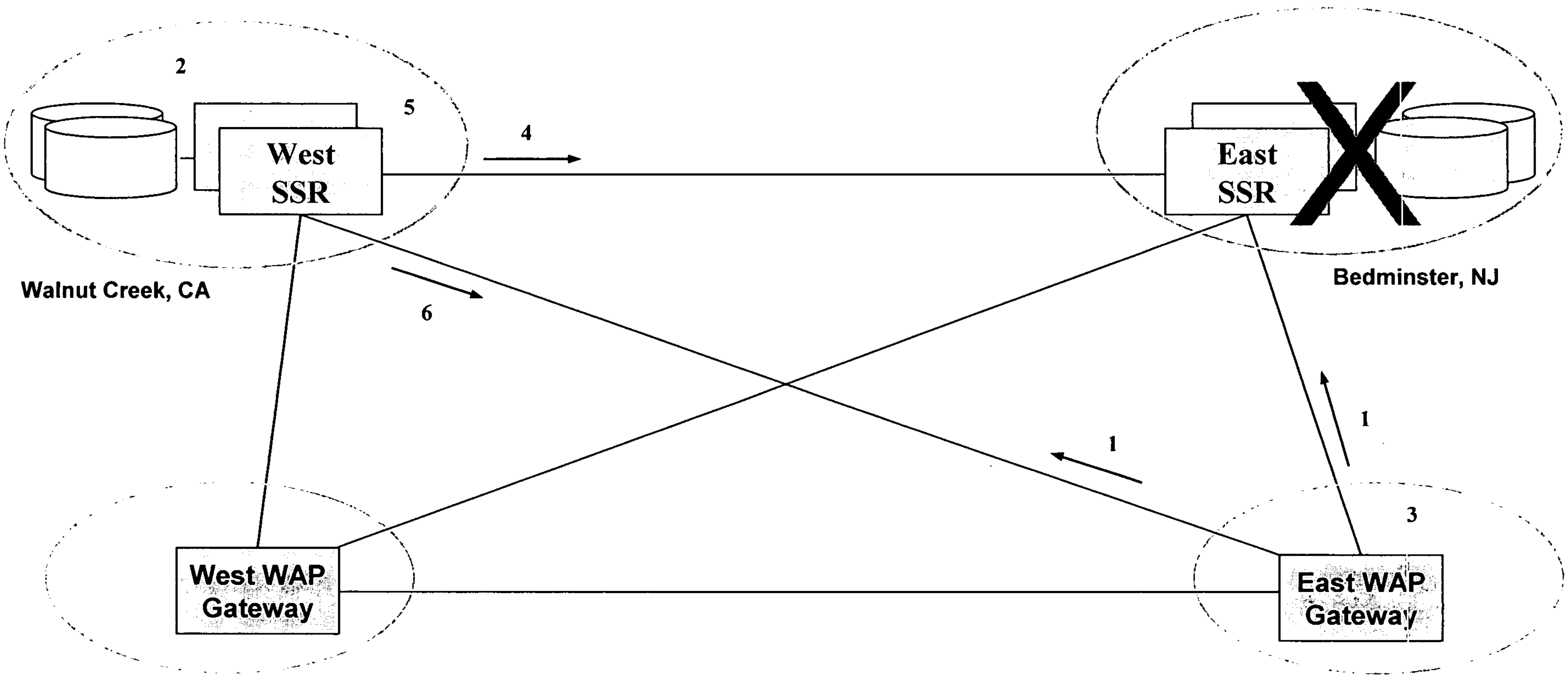
Alarming Queries – Link Down (Example: East WAP Gateway to East SSR)



1. WAP Gateways (East shown here) send LDAP queries, with known unsuccessful IP address, every X seconds to each SSR
2. West SSR searches locally for session record and doesn't find it
3. Query from East WAP Gateway to East SSR times out – ALARM
4. West SSR passes query to East SSR
5. If West SSR to East SSR link is good
   a) East SSR searches for session record and doesn't find it
   b) East SSR returns null response to West SSR
   c) West SSR returns null response to East WAP Gateway – NO ALARM (useful for troubleshooting)
6. If West SSR to East SSR link is bad
   a) Query from West SSR times out
   b) West SSR returns error to East WAP Gateway - ALARM

RESTRICTED AND PROPRIETARY
The information contained herein is for use by authorized Verizon Wireless employees with a need to know it and should not be disclosed to others.

Alarming Queries – SSR Down (Example: East SSR Down)



1. WAP Gateways (East shown here) send LDAP queries, with known unsuccessful IP address, every X seconds to each SSR
2. West SSR searches locally for session record and doesn't find it
3. Query from East WAP Gateway to East SSR times out or error is returned – ALARM
4. West SSR passes query to East SSR
5. Query from West SSR times out or error is returned
6. West SSR returns error to East WAP Gateway - ALARM

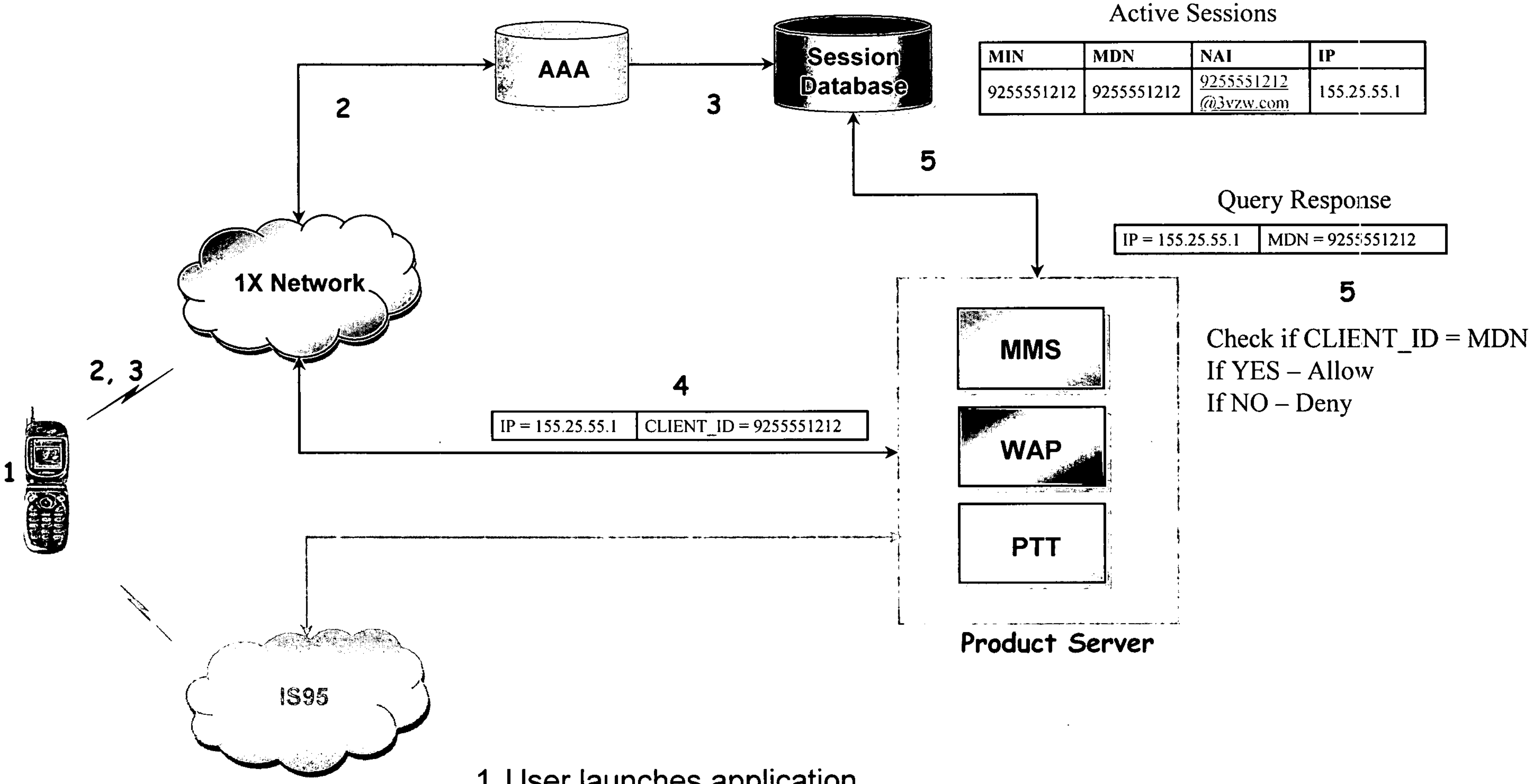
verizon wireless

Product Authentication
Roaming Issues

Network Technology Development
September 2, 2003

RESTRICTED AND PROPRIETARY
The information contained herein is for use by authorized Verizon Wireless & subsidiaries employees with a need to know it and should not be disclosed to others.

How it Works Today – Connection Over 1X



Active Sessions

MIN	MDN	NAI	IP
9255551212	9255551212	9255551212 @3vzw.com	155.25.55.1

Query Response

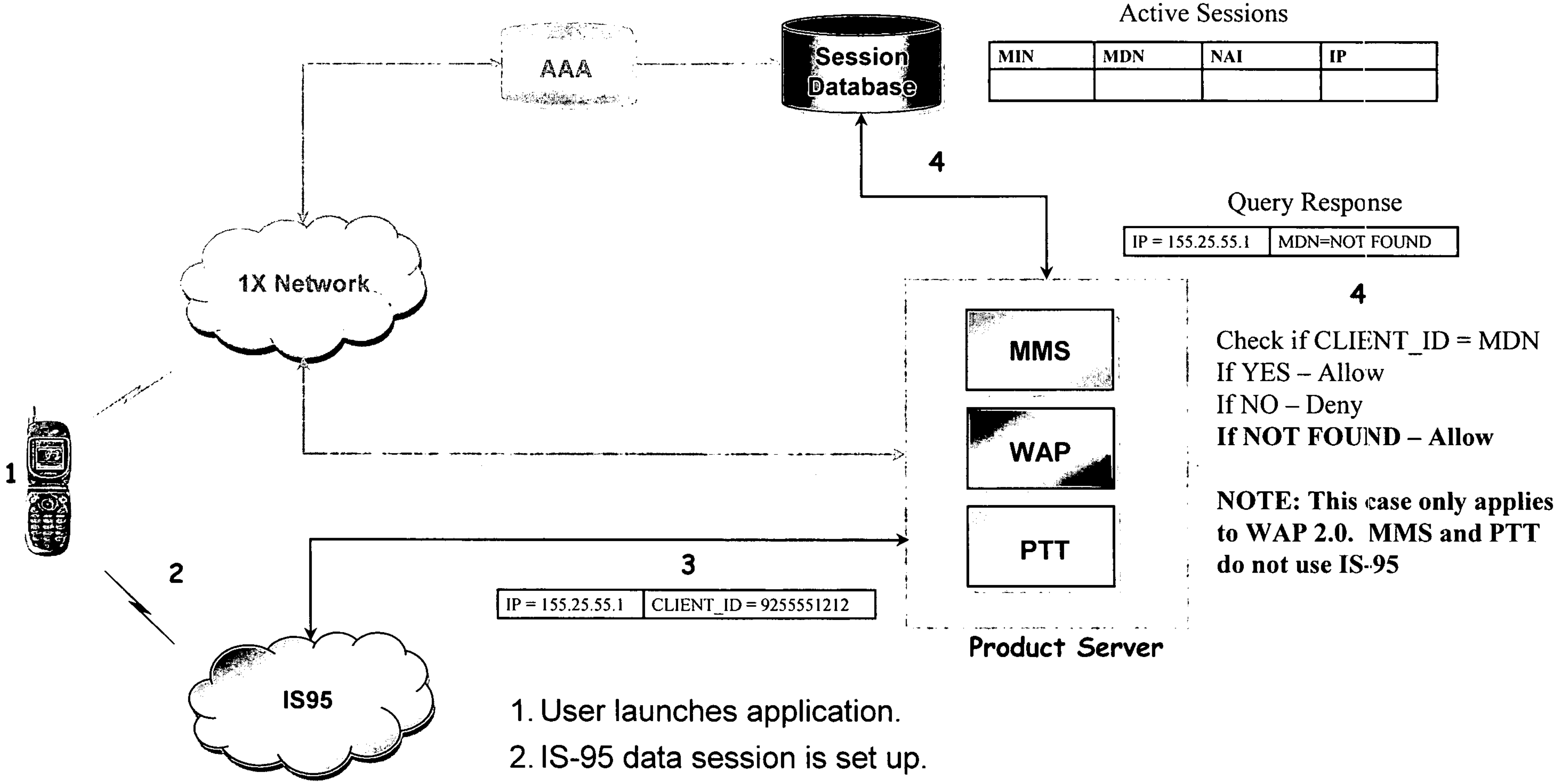
IP = 155.25.55.1	MDN = 9255551212

IP = 155.25.55.1	CLIENT_ID = 9255551212

Check if CLIENT_ID = MDN
If YES – Allow
If NO – Deny

1. User launches application.
2. 1X data session is set up after HLR & AAA authentication.
3. Record is added to Session Database
4. Client in the device presents its own identity to the product server.
5. Product server queries the AAA session database and authenticates the identity.

How it Works Today – Connection Over IS-95



Active Sessions

MIN	MDN	NAI	IP

Query Response

IP = 155.25.55.1	MDN=NOT FOUND

IP = 155.25.55.1	CLIENT_ID = 9255551212

4

Check if CLIENT_ID = MDN
If YES – Allow
If NO – Deny
If NOT FOUND – Allow

NOTE: This case only applies to WAP 2.0. MMS and PTT do not use IS-95

1. User launches application.
2. IS-95 data session is set up.
3. Client in the device presents its own identity to the product server.
4. Product server queries the AAA Session Database. Since IS-95 does not use the AAA, there is no record in the Session Database.

NOTE: Use of Session Database for IS-95:

- Requires implementation of double stack on IWF's
- Requires RADIUS interface with AAA
- Has been ruled out due to cost and IS-95 product life

RESTRICTED AND PROPRIETARY
The information contained herein is for use by authorized Verizon Wireless employees with a need to know it and should not be disclosed to others.

Summary of Current Product Authentication

- ○ 3G-1X Connections
  - — Will always have a record in the Session Database
  - — If a user attempts to spoof, then the Client ID from the device will not match the Session Database query and the user will be denied service
- ○ IS-95 Connections
  - — Will never have a record in the Session Database
  - — If a user attempts to spoof, there will not be a record in the Session Database the user will be allowed service
  - — Exposure: Users will only be successful spoofing when IS-95 connections are made. The user doing the spoofing will still be charged for the airtime. The only thing gained is access to the product server over IS-95.
  - — Since the product servers are protected behind VZW firewalls, users outside the VZW network will not get access.
- ○ Summary of Session Database Query Logic:
  - — If Client ID from device = MDN from the query – ALLOW SERVICE
  - — If Client ID from device is different than MDN from the query – DENY SERVICE
  - — If the query returns "Record Not Found" – ALLOW SERVICE (to allow IS-95 to work)
- ○ Summary of Exposure
  - — 1X subs – CANNOT SPOOF
  - — IS-95 subs – CAN SPOOF

Problem Scenario: CDMA Roaming

- 3G-1X Connections
  - VZW subscribers on foreign network
    - VZW firewalls must be opened to IP addresses from foreign network
    - Since AAA authentication is proxied back to VZW AAA, there WILL be a record in the Session Database
    - Data connection can be routed through the Internet to VZW product servers
    - If subscriber attempts to spoof, then the Client ID will not match the Session Database query, and the user will be denied service
  - Foreign roamers on VZW network
    - Since AAA authentication is proxied back to foreign AAA, there will NOT be a record in the VZW Session Database
    - If the subscriber attempts to spoof, then the Session Database will return "Record Not Found," and the product server will ALLOW service (same result as that for IS-95)
  - Foreign subscribers on foreign network
    - Since firewalls have been opened to IP addresses from foreign network, foreign subscribers can reach VZW product servers from their home network
    - If these subscribers attempt to spoof, then the Session Database will return "Record Not Found," and the product server will ALLOW service (same result as that for IS-95)
- IS-95 Connections
  - Same issue as today, but with the additional exposure of foreign subscribers on VZW network and foreign subscribers on their home network
- Summary of Exposure
  - VZW 1X subs on home or foreign network – CANNOT SPOOF
  - Foreign 1X subs on VZW network – CAN SPOOF
  - Foreign 1X subs on foreign network – CAN SPOOF
  - ALL IS-95 Subs – CAN SPOOF

Problem Scenario: GSM/GPRS Roaming

- GPRS Connections
  - VZW subscribers on foreign network
    - VZW firewalls must be opened to IP addresses from foreign network
    - If Inter-working Function proxies back to VZW AAA, there will be a record in the Session Database
    - Data connection can be routed through the Internet or through a tunnel back to VZW product servers
    - If subscriber attempts to spoof, then the Client ID will not match the Session Database query, and the user will be denied service
- 1X Connections
  - Foreign roamers on VZW network
    - Since AAA authentication is proxied back to VZW AAA, there will NOT be a record in the VZW Session Database
    - If the subscriber attempts to spoof, then the Session Database will return "Record Not Found," and the product server will ALLOW service (same result as that for IS-95)
  - Foreign subscribers on foreign network
    - Since firewalls have been opened to IP addresses from foreign network, foreign subscribers can reach VZW product servers from their home network
    - If these subscribers attempt to spoof, then the Session Database will return "Record Not Found," and the product server will ALLOW service (same result as that for IS-95)
    - GSM/GPRS network may provide mechanism to prevent all non-VZW subscribers to reach VZW product servers
- Summary of Exposure – as configured today
  - VZW GPRS subs on foreign network – CANNOT SPOOF
  - Foreign 1X subs on VZW network – CAN SPOOF
  - Foreign GPRS subs on foreign network – CAN SPOOF (unless GPRS network can block)

Solution #1: No Fallback to IS-95 (for WAP 2.0, MMS, and PTT)

- Change device requirements for WAP 2.0 to not allow fallback to IS-95 (MMS and PTT already do not fall back).
- Change Session Database query logic:
  - If Client ID from device = MDN from the query – ALLOW SERVICE
  - If Client ID from device is different than MDN from the query – DENY SERVICE
  - If the query returns “Record Not Found” – **DENY SERVICE**
- Pros
  - Solves authentication problem for roaming scenarios (both 1X and GPRS roaming)
  - Solves existing IS-95 security hole for non-roaming scenarios
- Cons
  - Change in device requirements could delay device availability
  - Products would not work in markets that don’t have 1X (same as MMS and PTT today)
  - Products would not work if device is unable to set up a 1X session

Solution #2: Deny IS-95 at the WAP 2.0 Gateway

- Change Session Database query logic to deny any connection where there is a “Record Not Found” in the Session Database
  - If Client ID from device = MDN from the query – ALLOW SERVICE
  - If Client ID from device is different than MDN from the query – DENY SERVICE
  - If the query returns “Record Not Found” – **DENY SERVICE**
  - Can create a user-friendly WML page to notify the user
- Pros
  - Solves authentication problem for roaming scenarios
  - Solves existing IS-95 security hole for non-roaming scenarios
- Cons
  - User-experience issues when legitimate user’s device attempts a IS-95 fallback connection
    - Setup time: All IS-95 fallback connections will go through session set up, access to gateway, and delivery/download of WML notification page
    - User is charged for the connection
    - Unnecessarily uses network resources
  - Products would not work in markets that don’t have 1X (same as MMS and PTT today)
  - Products would not work if device is unable to set up a 1X session